April 11, 2022

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

Re: Cybersecurity Risk Management for Investment Advisors, 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 comment on the above-captioned Proposed Rule ("Proposal" or "Release")[2] intended to enhance disclosure and resiliency in our financial markets. The Proposal has four components. It would require registered investment advisers and registered investment companies to adopt and implement cybersecurity risk management policies and procedures; it would require registered investment advisors to report cybersecurity incidents to the Securities and Exchange Commission ("Commission"); it would enhance disclosures to clients and investors by registered investment advisers and registered investment companies related to cybersecurity risks and incidents; and it would require registered investment advisers and registered investment companies to maintain books and records related to cybersecurity.

All four components of the Proposal are important to protecting investors' personal identifiable information and funds from cyberattacks, enhancing the resiliency of the financial system, and promoting investor confidence in our financial markets. For example, the Proposal includes a flexible cybersecurity framework that requires all advisers and funds to adopt and implement cybersecurity policies and procedures to protect clients and investors against cyberattacks. As the Commission finalizes the Proposal, it should resist pressure to dilute its provisions. In particular, the Proposal should apply to all registered investment advisers and registered investment companies broadly, without carveouts for asset thresholds or differing fund

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 87 Fed. Reg. 13,524 (Mar. 9, 2022).

structures. In addition, the final rule should include a number of enhancements. The Proposal's requirement for incident reporting to the Commission within 48-hours of learning of a cyberattack will enable the Commission to monitor and respond to cybersecurity threats industry-wide that may pose risks to financial stability. However, that time period should be shortened to 24 hours. Similarly, the Proposal's enhanced disclosures of cybersecurity risks and incidents faced by advisers and funds will serve to further educate clients and investors about where to invest their funds, but the Commission should consider additional disclosures to assist clients and investors in making more informed investment decisions.

## BACKGROUND

Testifying before the U.S. Senate Committee on Homeland Security and Governmental Affairs last year, the Director of the agency charged with managing and mitigating cybersecurity risks to critical infrastructure, the Cybersecurity and Infrastructure Security Agency ("CISA"), stated that the U.S. is facing "unprecedented risk from cyberattacks undertaken by both nation-state adversaries and criminals."[3] The rise in the sheer number of cyberattacks and their growing sophistication has led many, both inside and outside the government, to acknowledge cybersecurity threats as one of the top risks facing the private sector. In the World Economic Forum's Global Risks Perception Survey, respondents cited cyberattacks and data fraud or theft as two of the top five global risks, compared to the same survey from ten years earlier where neither were mentioned among the top five global risks.[4] Further, malware and ransomware attacks in 2020 increased by 358% and 435%, respectively from the previous year.[5] This trend shows little sign of abating in the near future as businesses become more dependent on digitizing their operations and storing more and more valuable data within their networking systems. This all serves as further motivation and riper targets for cybercriminals to monetize cyberattacks.

For each data breach, experts have estimated that the average cost per record breached was $161 in 2021, a 14.2% increase since 2017.[6] While $161 per record may not seem like a large sum of money on its own, cybercriminals are less likely to target individuals, and are more likely to target businesses and organizations with vast troves of data representing thousands and millions of records. This number also does not account for the financial damage wreaked on the individual consumer or investor who has had their sensitive information breached, which can be debilitating and devastating. In the case of large breaches, the financial damage of a cyberattack or data breach can have consequential and systemic consequences not only in the markets but also on society as a whole. Below are just a few examples of how past cyberattacks and data breaches can impact the economy:

---

3 *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Committee on Homeland Security & Governmental Affairs*, 117th Cong. (2021) (statement of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency).

4 WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 8 (2019), https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

5 *Id.* at 9.

6 IBM, COST OF A DATA BREACH REPORT 13 (2021), https://www.ibm.com/downloads/cas/OJDVQGRY.

- In 2014, the internet company, **Yahoo! Inc.**, experienced a major cyberattack and data breach that compromised information from more than 500 million user accounts, including names, email addresses, telephone numbers, dates of birth, and more. Despite its knowledge of the data breach in 2014, Yahoo did not disclose the breach to investors for nearly two years. The day after the announcement, Yahoo! Inc.'s stock price fell by 3% and its market capitalization fell by $1.1 billion. In 2018, the company settled SEC charges that it misled investors by failing to disclose the breach and paid a penalty of $35 million.[7]

- In 2017, the credit reporting company, **Equifax**, experienced a major cyberattack and data breach that compromised information from more than 147 million people due to failure to implement a critical network patch after being alerted of a security vulnerability in their database. This data breach exposed 145.5 million Social Security numbers and 209,000 payment card numbers. In a settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories, the company agreed to pay up to $700 million in penalties and restitution for its failures to adequately safeguard user data.[8]

- In 2019, cybercriminals breached the network management company, **Solarwinds**, which monitors network activity for its customers, including various departments across the federal government. The hackers were able to infiltrate Solarwinds' networks and inject hidden code into software updates the company was providing to customers, which effectively opened a back-door for the hackers to enter customers' networks, including the federal government. The hackers had access to sensitive data for more than a year before the company or its customers became aware.[9]

- In 2021, the largest gas pipeline operator in the U.S., **Colonial Pipeline**, which provides the east coast with 45% of its gas, paid a $4.4 million ransom to restore operations after hackers were able to penetrate its networks through a leaked virtual private network login password.[10] During the several days the pipeline was

---

7 Altaba Inc., No. 3-18448 (Securities Exchange Commission April 24, 2018).

8 Press Release, Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach.

9 Government Accountability Office, *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response*, WatchBlog (April 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

10 *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Committee On Homeland Security & Governmental Affairs*, 117th Cong. (2021) (statement of Joseph A. Blount, Jr., President and Chief Executive Officer, Colonial Pipeline).

shutdown, gas prices spiked seven cents and led to gas stations running out of gas at roughly 1,800 locations nationwide.[11]

- In 2021, the largest meat processing plant in the U.S., **JBS USA Holdings Inc.**, which provides roughly one-fifth of the U.S.'s meat supply, paid an $11 million ransom to hackers after they infiltrated their networks.[12] As a result of JBS shuttering operations for two days, the CME Lean Hog and Live Cattle prices moved sharply lower.[13]

The COVID-19 pandemic and the changes in the modern workplace that have come as a result of the pandemic have only elevated the risk of cyberattacks. The increase in remote work has made companies and organizations more vulnerable to cyberattacks through increased usage of teleworking strategies, including virtual meeting applications and virtual private networks.[14] Research has found that data breaches where remote work was a factor in the breach increased the total cost of a breach by $1.07 million on average.[15] This raises the level of vigilance that all market participants must maintain in connection with cybersecurity vulnerabilities and further demonstrates the growing risk cybersecurity poses to society.

The financial industry and its participants are not immune or insulated from the growing risk of cyberattacks and data breaches. Why? Chairman Gensler summed it up in a speech earlier this year on cybersecurity and securities law when he cited a quote by the infamous bank robber Willie Sutton when asked why he robbed banks: "Because that's where the money is."[16] In fact, the average cost to a financial services company of a cyberattack is 40% higher than the average cost to companies in other sectors.[17] As the financial services industry is a natural target for cyberattacks, the Financial Stability Oversight Council ("FSOC") has increasingly discussed cyberattacks as a threat to the stability of the U.S. financial system in their annual reports to Congress, stating "incidents have the potential to impact tens or even hundreds of millions of Americans and result in financial losses of billions of dollars due to disruptions in operations, theft, and recovery costs."[18] FSOC goes on to highlight three channels through which financial stability could be threatened: 1) disruption of a key financial service or utility with little or no substitute; 2) compromised integrity of market data; and 3) loss of consumer or investor confidence in markets

---

11 Kate Gibson, Megan Cerullo, *Gas shortages worsen as fuel prices spike after Colonial Pipeline ransomware attack*, CBS NEWS (May 13, 2021, 3:17 PM), https://www.cbsnews.com/news/gas-prices-shortages-worsen-colonial-pipeline-ransomware-attack/.

12 Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, Wall Street Journal (Jun. 9, 2021, 8:27 PM), https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781?mod=hp_lead_pos2.

13 FINANCIAL STABILITY OVERSIGHT COUNCIL (FSOC), ANNUAL REPORT 62 (2021).

14 *Id.* at 16.

15 IBM, *supra* note 6.

16 Gary Gensler, Chairman, Securities Exchange Commission, Cybersecurity and Securities Laws (Jan. 24, 2022) (quoting Federal Bureau of Investigation, "Willie Sutton," https://www.fbi.gov/history/famous-cases/willie-sutton).

17 ANDREW P. SCOTT AND PAUL TIERNO, CONG. RSCH. SERV., IF11717, INTRODUCTION TO FINANCIAL SERVICES: FINANCIAL CYBERSECURITY (Jan. 13, 2022), https://crsreports.congress.gov/product/pdf/IF/IF11717.

18 FSOC, *supra* note 13 at 168.

that affects the safety and liquidity of assets.[19] To improve cybersecurity resiliency in the financial sector, FSOC recommended that regulators monitor cybersecurity risks through examinations at financial institutions and improve information sharing between private and public sectors, specifically as it relates to cyberattack incident reporting.[20] Federal financial regulators across the federal government have responded by elevating cybersecurity issues to the top of their rulemaking agenda in recent years.[21]

## OVERVIEW OF THE PROPOSAL

The Commission has proposed several new rules and rule amendments under the Investment Advisers Act of 1940 and Investment Company Act of 1940 governing cybersecurity risk management policies and procedures, enhanced disclosure of cybersecurity risks and incidents to clients and customers, and incident reporting to the Commission by registered investment advisers and registered investment companies. Specifically, the SEC's proposed rule would:

- implement new rules 206(4)-9 under the Investment Advisers Act and 38a-2 under the Investment Company Act, which would require registered investment advisers and registered investment companies to adopt and maintain cybersecurity policies and procedures;

- require registered investment advisers to submit a new Form ADV-C to report significant cybersecurity incidents to the Commission within 48 hours after having a reasonable basis to conclude such an incident occurred;

- amend Form ADV Part 2A to require registered investment advisers to promptly disclose cybersecurity risks and incidents to existing and prospective clients;

- require registered investment companies to promptly disclose to current and prospective investors cybersecurity risks and significant cybersecurity incidents that occurred in the previous two fiscal years in funds' registration statements;

- amend Rule 204-2 under the Investment Advisers Act and Rule 38a-2 under the Investment Companies Act to ensure books and records rules are maintained in connection with cybersecurity risk management policies and incidences.

---

19 *Id.* at 168–169.

20 *Id.* at 170.

21 *See* Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,272 (Dec. 09, 2021) (to be codified at 16 C.F.R. § 314) (extended Safeguard rules related to data security to non-bank financial institutions); s*ee* Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021) (requires banking organizations to notify their primary regulator of a cyber incident within 36 hours).

## COMMENTS

### I. THE PROPOSAL WILL ENHANCE INVESTOR PROTECTION AND CONTRIBUTE TO FINANCIAL STABILITY AND SHOULD NOT BE DILUTED BY SPECIOUS INDUSTRY CONCERNS.

Broadly speaking, enhancing the cybersecurity resiliency of our financial markets and increasing transparency into the cybersecurity risks facing registered investment advisers and registered investment companies are desperately needed in today's digital economy. The Proposal would advance both of these goals by ensuring advisers and funds are properly mitigating the risks associated with cyberattacks and data breaches, safeguarding investors' data and funds, and increasing information sharing between the private and public sectors to mitigate systemic risk.

This Proposal correctly notes that there are currently no rules that require advisers and funds to adopt and implement a comprehensive cybersecurity program.[22] This regulatory gap poses unnecessary risks to investors and the stability of our financial markets more broadly. As the Commission points out, clients and investors will be significantly more protected against cyberattacks and data breaches if advisers and funds are required to adopt and maintain cybersecurity policies and procedures.[23] The Proposal's incident reporting requirement will also bolster the Commission's ability to protect investors, market participants, and the financial markets.[24] It will allow the Commission to ensure advisers and funds are complying with their fiduciary responsibilities to clients and investors before a cyberattack, and it will enable the Commission, after a cyberattack, to take remedial action against advisers who have breached their fiduciary responsibilities to safeguard funds. More broadly, the Proposal will help the Commission monitor the markets for systemic risks posed by cyberattacks and data breaches. The Proposal thus enhances investor protection and contributes to financial stability.

The Commission should not dilute the Proposal on the basis of specious industry concerns. The Commission should be especially wary of arguments from industry that it should carve out specific advisers or funds or otherwise dilute the effectiveness of the Proposal to reduce the burden on the industry. The financial industry often seeks to weaken or eliminate regulations by arguing that the requirements will have a devastating impact on their business, which will in turn harm the public interest and even investors.[25] These sorts of claims are typically exaggerated if not groundless.[26] For example, commenters have already urged the Commission to exempt advisers with assets under $100 billion or some other specific threshold.[27] The Proposal, as currently

---

22 Release at 13,527.

23 Release at 13,525.

24 Release at 13,526.

25 *See, e.g.,* Marcus Baram, *The Bankers Who Cried Wolf: Wall Street's History of Hyperbole About Regulation*, Huffington Post (Jun. 21, 2011), https://www.huffpost.com/entry/wall-street-history-hyperbole-regulation_n_881775.

26 *Id.*

27 Adrian Day, Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies, and Business Development Companies (Mar. 09, 2022), https://www.sec.gov/comments/s7-04-22/s70422-20117386-268668.htm; *see* Anonymous, Comment Letter on Cybersecurity Risk Management for

drafted, is sufficiently flexible to enable advisers and funds of all sizes to comply and better safeguard their clients' and investors' investments because the framework is risk-based, as opposed to one-size-fits-all. It would be particularly misguided for the Commission to carve out specific advisers or funds from compliance with the Proposal because it would create blind spots in the Commission's ability to effectively monitor the market for cyberattacks and data breaches that could threaten financial stability. Additionally, if specific advisers or funds were carved out from the requirement to adopt and maintain cybersecurity policies and procedures, it could have an adverse effect by incentivizing cybercriminals to target those more vulnerable advisers and funds, specifically because they would be less likely to have effective cybersecurity policies and procedures and incident reporting requirements in place.

## II. THE PROPOSAL'S RISK MANAGEMENT FRAMEWORK STRIKES THE RIGHT BALANCE BETWEEN FLEXIBILITY AND ENSURING CYBERSECURITY RESILIENCY IN OUR FINANCIAL MARKETS.

The Proposal's risk management rules enumerate core cybersecurity risk management measures to enhance resiliency in our financial markets, while also providing enough flexibility that they can apply to all registered investment advisers and all registered investment companies. The Commission's proposed risk management rules are rightfully based on other cybersecurity frameworks established elsewhere in the public sector.[28] The Proposal requires several elements to be included in advisers' and funds' policies and procedures: risk assessment, user security and access, information protection, threat and vulnerability management, cybersecurity incident response, and recovery.[29] It also includes important oversight elements to ensure the policies and procedures are being adhered to and continually reviewed, including requiring annual review and written reports, fund board oversight, and certain recordkeeping requirements. Collectively, the Proposal's cybersecurity risk management rules, if followed, will prove critical to advisers' and funds' ability to better protect client and investor assets from cyberattacks and data breaches in the future.

The Commission should reject any argument that compliance with already existing cybersecurity frameworks should serve as a safe harbor for compliance with the Proposal. The Proposal's policies and procedures for cybersecurity risk management advance the Commission's unique mission to "protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation"[30] While several other cybersecurity frameworks were referenced as a basis for the framework in this Proposal, they were not created with the Commission's mission and directives from Congress in mind. The Commission must adopt and enforce the Proposal's specific

---

Investment Advisors, Registered Investment Companies, and Business Development Companies (Mar. 09, 2022), https://www.sec.gov/comments/s7-04-22/s70422-20118967-271795.htm.

28 See CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, CYBER ESSENTIALS STARTER KIT – THE BASICS FOR BUILDING A CULTURE OF CYBER READINESS (Spring 2021), cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf; *see* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, (Apr. 16, 2018).

29 *See* Release at 13,529 – 13,533.

30 Securities and Exchange Act, 15. U.S.C. § 78a (1934).

cybersecurity risk management policies and procedures because they advance the Commission's specific mission. Therefore, it is critically important the Commission reject any argument that compliance with existing cybersecurity frameworks should serve as a safe harbor for compliance with this Proposal.

Oversight and approval of a fund's cybersecurity policies and procedures by the fund's board of directors is critical and consistent with their existing responsibilities. The Proposal requires a fund's board of directors to approve cybersecurity policies and procedures, review an annual report on any material changes to the policies and procedures, and review past cybersecurity incidents.[31] This is a vital part of the Proposal that should not be altered. Due to the rising cases of cyberattacks and rising level of sophistication of attacks, the financial impacts of a cyberattack or data breach are so great that a fund's board of directors must have direct knowledge and approval of a fund's cybersecurity policies and procedures. The Commission should reject any argument that seeks to insulate a fund's board of directors from its duty to oversee adoption and implementation of cybersecurity policies and procedures.

## III. THE PROPOSAL'S 48-HOUR REQUIREMENT FOR INCIDENT REPORTING BY REGISTERED INVESTMENT ADVISERS SHOULD BE STRENGTHENED.

The Proposal's 48-hour cybersecurity incident notification threshold for reporting significant cybersecurity incidents to the Commission affecting the adviser or its fund will enable the Commission to better assess potential systemic risks affecting the market, but it should be made more effective by shortening the mandatory reporting window to 24 hours. As the Commission correctly points out, this provision would not only enable the Commission to monitor and evaluate the effects of a single cyberattack and data breach on individual advisers to ensure investors are being protected, but equally important, this provision would also allow the Commission to monitor specific incidents to assess potential systemic risks affecting financial markets.[32] The Proposal further states the 48-hour incident reporting requirement would "give an adviser time to confirm its preliminary analysis, and prepare the report while still providing the Commission with timely notice about the incident."[33] As discussed above, risks to financial stability posed by cyberattacks and data breaches are rising in number and sophistication with no signs of slowing down. It is critically important for regulators and the private sector to engage in information sharing during cybersecurity incidents as quickly as possible. We therefore urge the Commission to consider shortening the incident reporting threshold from 48 hours to 24 hours.

As mentioned above, CISA, an agency located within the U.S. Department of Homeland Security, is responsible for leading the nation's cybersecurity response and protecting against critical infrastructure risks posed by cyberattacks and data breaches. As the nation's lead agency for defending critical infrastructure from cyberattacks and data breaches, the head of that agency, the Director, is one of the foremost experts in the U.S. government on best practices for guarding

31 Release at 13,534.
32 Release at 13,536.
33 Release at 13,537.

against cyberattacks and data breaches. While testifying before Congress, the Director stated in her written testimony:

> "[t]he earlier that CISA, the Federal lead for asset response, receives information about a cyber incident, the faster we can conduct urgent analysis and share information to protect other victims. To that end, cyber incident reporting must be timely, ideally within 24 hours of detection."[34]

This is persuasive evidence that the 24-hour notification deadline is necessary and appropriate to optimize the effectiveness of the Proposal.

As the Commission points out, cybersecurity incident reporting to the Commission would help assess the potential systemic risks that any one incident could pose to the financial markets more broadly.[35] The Commission recognizes that incident reporting can not only enhance the agency's ability to ensure investors are protected when individual advisers and funds experience cyberattacks and data breaches but also can assist staff in identifying patterns and trends that pose threats across the industry, information that could help protect other market participants from similar attacks.[36] If one of the goals of the Proposal is to allow the Commission to best monitor cyber risks across registrants to protect against industrywide cyberattacks that threaten financial stability, the earlier the Commission can receive cybersecurity incident reports from advisers, the more effectively they can accomplish that goal.

In fact, the Commission has already set a precedent for a 24-hour incident reporting threshold in Reg SCI.[37] In the final rule, the Commission rejected arguments from commentors to extend the 24-hour incident reporting threshold to 48 hours or later, stating:

> "[t]he Commission continues to believe that Rule 1002(b)(2)'s requirement to provide information to the Commission within 24 hours is appropriately tailored to help the Commission and its staff quickly assess the nature and scope of an SCI event and will contribute to more timely and effective Commission oversight…"[38]

In short, the Commission should follow the guidance of the Director of CISA when she stated that in order to protect other potential victims, incident reporting should ideally be within 24 hours. Further, the Commission should adhere to its own precedent for a 24-hour incident reporting requirement, established in its Reg SCI rulemaking. For these reasons, we urge the

---

34 *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Committee on Homeland Security & Governmental Affairs*, 117th Cong. (2021) (statement of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency).

35 Release at 13,527.

36 Release at 13,536.

37 Systems Compliance and Integrity, 17 C.F.R. Subpart 0.

38 Regulation Systems Compliance and Integrity, 79 Fed. Reg. 72,252, 72,327 (Dec. 5, 2014).

Commission to shorten the time period for cybersecurity incident reporting to the Commission from 48 hours to 24 hours.

## IV. THE PROPOSAL'S ENHANCED DISCLOSURE REPORTING TO CURRENT AND PROSPECTIVE CLIENTS AND INVESTORS INCREASES INVESTOR PROTECTION BUT SHOULD INCLUDE ADDITIONAL DISCLOSURES.

The Proposal's enhanced disclosure reporting to current and prospective clients and investors serves to increase investor protection, but it could and should be further enhanced with additional important disclosures. Broadly speaking, the SEC's disclosure regime is critical to the trust that upholds the U.S. capital markets. As one commentator has pointed out, "[i]nvestor trust is therefore critical for the securities markets to work, and disclosure helps to facilitate that trust. Ultimately, disclosure decreases investor risks and protects the public interest."[39] In other words, a robust disclosure regime is essential to the proper functioning of the securities markets; investors must know that the law requires meaningful and accurate disclosures and that failure to provide them will result in meaningful enforcement actions to punish and deter wrongdoers.

The Commission is rightfully concerned about the effectiveness of current disclosures by advisers and funds to clients and investors related to cybersecurity risks and incidents.[40] In fact, the Commission recently sanctioned eight firms for failures in their cybersecurity policies and procedures after a data breach that resulted in the theft of personal identifiable information of thousands of customers and clients.[41] In that order, the Commission found several of the advisers failed to establish cybersecurity policies and procedures after a cyberattack had occurred and misled clients to believe incident "notifications were issued much sooner than they actually were after discovery of the incident."[42] This is further evidence that the current ad hoc reporting and disclosure system for cyberattacks and data breaches needs more uniformity across the industry Based on filings with the Commission, there are more than 14,000 advisers with $113 trillion in assets under management, including 55% that serve custodial functions for their clients totaling $39 trillion.[43] With that many advisers in charge of that much money, it is essential that investors and clients be informed about an adviser's or fund's cybersecurity policies and procedures and past cybersecurity incidents before entrusting their money to those advisers or funds.

The Proposal's requirement for advisers and funds to "promptly" disclose cybersecurity incidents is vague and therefore creates too much leeway for advisers and funds to delay disclosing these important incidents. As the Commission has seen with other requirements in securities laws for "prompt" reporting and disclosure requirements, advisers and funds will take full advantage of that discretion if permitted. For example, the Commission's recently proposed rule regarding beneficial ownership proposes to revise the requirement that market participants file Schedule 13G

---

39 Susanna Kim Ripken, *The Dangers and Drawbacks of the Disclosure Antidote: Toward A More Substantive Approach to Securities Regulation*, 58 BAYLOR L. REV. 139, 155 (2006).

40 Release at 13,525.

41 Press Release, Securities and Exchange Commission, SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169.

42 *Id.*

43 Release at 13,547.

amendments "promptly" to a specified deadline of one business day.[44] The Commission's reasoning for the change was to "remove any uncertainty as to the date on which an amendment is due and help ensure that beneficial owners amend their filings in a more uniform and consistent manner."[45] The Commission's reasoning for eliminating that "promptly" standard in favor of a more certain time period applies equally to this Proposal. Moving forward with the Proposal's requirement for advisers and funds to disclose cybersecurity incidents to clients and advisors "promptly" will invite abuse and delay by market participants. Therefore, the Commission should specify a deadline for disclosure to clients and investors, including a "no later than" requirement.

The Commission should also require additional disclosures to prospective and current clients and investors that would better help them assess advisers' and funds' cybersecurity risks and defensive capabilities. Drawing from the general rationale for the Commission's disclosure regime, the Proposal's goal of including these disclosures to current and prospective clients and investors is to "enhance investor protection…to increase understanding in these areas and help ensure that investors and clients can make informed investment decisions."[46] In light of these goals, the Commission should require additional disclosures to better equip investors and clients to make more informed investment decisions, including disclosure of:

- any ransom payments made in connection with a cyberattack in the previous two fiscal years;
- whether the adviser or fund provides annual cybersecurity training to employees; and
- whether their cybersecurity policies and procedures are audited by a third party.

These additional disclosures by advisers and funds will further the Proposal's goal of increasing understanding regarding cybersecurity risks of investing with specific advisers and funds and helping investors and clients make more informed investment decisions.

## V. THE COMMISSION SHOULD CONSIDER THE PROPOSAL TO BE MERELY A FIRST STEP IN ADDRESSING CYBERSECRUITY WITHIN OUR FINANCIAL MARKETS.

As pointed out above, the Proposal will enhance investor protection and contribute to financial stability by making registered investment advisers and registered investment companies more resilient to cyberattacks and data breaches. However, the Proposal represents a necessary, but not sufficient, step in addressing the risks posed by cyberattacks and data breaches to our financial markets more broadly. The Commission should continue its work to advance this Proposal in concert with other cybersecurity initiatives, including continuing its work to finalize

44 Modernization of Beneficial Ownership, 87 Fed. Reg. 13,846 (Mar. 10, 2022).
45 *Id.* at 12,857.
46 Release at 13,527.

already proposed rules that extend Reg SCI to more market participants;[47] requiring uniform cybersecurity disclosure by publicly traded companies;[48] and proposing new cybersecurity rules to modernize Reg S-P and extend cybersecurity requirements to third-party service providers. These actions, taken together, will help to knit together a more resilient cybersecurity framework across out financial markets that better protects investors, advances financial stability, and instills confidence in our markets, both domestically and internationally.

## CONCLUSION

We hope these comments are helpful as the Commission finalizes the Proposal.

Sincerely,

Stephen W. Hall
Legal Director and Securities Specialist

Scott Farnin
Legal Counsel

Better Markets, Inc.
1825 K Street, NW
Suite 1080
Washington, DC 20006
(202) 618-6464

[redacted]

http://www.bettermarkets.org

47 Amendments Regarding the Definition of "Exchange" and ATSs That Trade U.S. Treasury and Agency Securities, NMS Stocks, and Other Securities, 87 Fed. Reg. 15,496 (Mar. 18, 2022).

48 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590 (Mar. 23, 2022).