June 5, 2023

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. 20,212 (Apr. 5, 2023)

Dear Ms. Countryman:

Better Markets[1] appreciates the opportunity to comment on the above-captioned Proposed Rule ("Proposal" or "Release")[2] intended to enhance cybersecurity disclosure and resiliency in our financial markets. The Proposal has four primary components. It would require certain market entities to 1) establish, maintain, and enforce cybersecurity policies and procedures and review the design and effectiveness of those policies and procedures on an annual basis; 2) report significant cybersecurity incidents to the Securities and Exchange Commission ("Commission") on Part I of proposed Form SCIR; 3) publicly disclose summary descriptions of their cybersecurity risks and significant cybersecurity incidents experienced during the previous or current calendar year on Part II of proposed Form SCIR; and 4) maintain books and records related to cybersecurity.

All four components of the Proposal are necessary for the Commission to carry out one of its core mission objectives, which is maintaining fair, orderly, and efficient markets. For example, the Proposal includes a cybersecurity risk management framework that requires all market entities that perform critical services to adopt and implement cybersecurity policies and procedures that

---

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 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, 88 Fed. Reg. 20,212 (Apr. 5, 2023).

are tailored to their unique risks. Additionally, the Proposal requires certain market entities to immediately report significant cybersecurity incidents to the Commission and update the Commission on a regular basis to ensure the integrity and functioning of the financial markets.

As the Commission finalizes the Proposal, it should resist pressure to dilute its provisions. In particular, 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 requirements for cybersecurity risk management advance the Commission's unique and vital mission to maintain orderly markets, and other frameworks, while valuable, are no substitute for the measures in the Proposal. In addition, the final rule should include a number of enhancements. The Proposal should require stricter board oversight of cybersecurity policies and procedures as well as increased disclosures on proposed Form SCIR that include information such as whether or not a market entity has paid a ransom related to a cybersecurity incident; whether or not a market entity has a designated Chief Information Security Officer; and whether or not a market entity has an independent, third-party audit conducted on their cybersecurity policies and procedures.

BACKGROUND

Speaking on the topic of cybersecurity in 2012, former Federal Bureau of Investigation Director Robert Mueller said "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[3] The former FBI Director's words are just as true now, if not more so, than they were back in 2012. While technology has revolutionized the way corporations conduct business, it has not come without its own set of risks and vulnerabilities. A 2019 survey of cybersecurity professionals reinforces the former FBI Director's statement, with almost half of respondents reporting an increase in cyberattacks on their organization and 79 percent reporting they expect to experience a cyberattack next year.[4] The question of whether or not a company will experience a cyberattack is becoming less a matter of "if" it will happen and more of a matter of "when" it will happen and how much damage will it cause.

The rise in the sheer number of cyberattacks and their growing sophistication has led many to acknowledge cybersecurity threats as one of the top risks facing the private sector. In the World Economic Forum's 2019 Global Risks Perception Survey, respondents cited cyberattacks and data fraud or theft as two of the top five global risks.[5] This is in stark contrast with the results from the same survey conducted ten years earlier, which mentioned neither cyberattacks nor data fraud

---

3 Robert S. Mueller, Director, FBI, RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

4 Press Release, Information Systems Audit and Control Association, New Study Reveals Cybercrime May Be Widely Underreported – Even When Laws Mandate Disclosure (June 3, 2019), New Study Reveals Cybercrime May Be Widely Underreported Even When Laws Mandate Disclosure (isaca.org).

5 World Economic Forum, The Global Risks Report 8 (2019), https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

among the top five global risks. To help put the perceived risks surrounding cybersecurity into context with other risks posed to companies, the PricewaterhouseCoopers' 2022 Annual Global CEO Survey found that cybersecurity edged out the COVID-19 global health crisis as the threat CEOs are most worried about over the next 12 months.[6] That point bears repeating—CEOs viewed the potential threat of a cyberattack or data breach to be a greater threat to their company in 2022 than the risk posed by a global pandemic, a pandemic that has unfolded over several years and exacted a huge toll in human life and economic damage.

Just as we have seen the economic damage a global pandemic can have on companies of all sizes, we have also seen the crippling effects a major cyberattack or data breach can have on a company. For example, we saw the largest gas pipeline operator and the largest meat processing plant in the U.S. each forced to halt operations due to a pair of cyberattacks in 2021. These cyberattacks cut off 45% of the oil to the East Coast and halted production at a company that provides one-fifth of the U.S.'s meat supply.[7] In addition, malware and ransomware attacks increased in 2020 by 358% and 435%, respectively, from the previous year.[8] When you combine the debilitating consequences of a successful cyberattack, combined with the relentless threat of attack, it is no wonder cybersecurity is the top threat to U.S. companies cited by CEOs. Unfortunately, this trend can be expected to increase as businesses become more dependent on digitizing their operations and storing more and more valuable data within their networking systems. This increased reliance on digitized data will create increasingly attractive targets for cybercriminals, motivating them to ramp up their cyberattacks.

For each data breach, experts have estimated that the average cost *per record* breached was $164 in 2022, a 16.3% increase since 2017.[9] While $164 per record may not seem like a large sum of money in isolation, it actually suggests huge collective costs, as cybercriminals are less likely to target individuals and more likely to target businesses and organizations with vast troves of data representing thousands and millions of records. The average cost of a data breach in the United States in 2022 was $9.44 million, while the average cost of a ransomware attack in 2022, prior to any ransom being paid, was $4.54 million.[10] 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.

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 use of teleworking strategies, including virtual meeting applications and virtual private networks.

---

6 PricewaterhouseCoopers, *Reimagining the outcomes that matter* (Jan. 17, 2022), https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html.

7 *See* Financial Stability Oversight Council, Annual Report 62 (2021).

8 World Economic Forum, *supra* note 5 at 9.

9 IBM, Cost of a Data Breach Report 9 (2022), https://www.ibm.com/downloads/cas/3R8N1DZJ.

10 *Id.* at 6-7.

Research has found that data breaches where remote work was a factor in the breach increased the total cost of a breach by nearly $1million on average.[11] 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 last year on cybersecurity and securities law when he cited a quote from the infamous bank robber Willie Sutton when he was asked why he robbed banks: "Because that's where the money is."[12] 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.[13] 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."[14] 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 that affects the safety and liquidity of assets.[15]

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.[16] Federal financial regulators across the federal government have responded by elevating cybersecurity issues to the top of their rulemaking agenda in recent years.[17]

---

11 *Id.* at 6.

12 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).

13 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. \

14 FSOC, *supra* note 7 at 168.

15 *Id.* at 168–169.

16 *Id.* at 170.

17 *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).

OVERVIEW OF THE PROPOSAL

The Commission has proposed new Rule 10 and new Form SCIR to require Market Entities, defined in the Proposal, to establish, maintain, and enforce written cybersecurity risk management policies and procedures. The proposed new Rule 10 also establishes an incident reporting framework to the Commission for significant cybersecurity events. Covered Entities, as defined by the Proposal, would be subject to additional requirements under proposed Rule 10.

Market Entities

"Market Entities" include the following entities regulated by the Commission:

- broker-dealers
- broker-dealers that operate an alternative trading system
- clearing agencies
- major security-based swap participants
- Municipal Securities Rulemaking Board
- national securities associations
- national securities exchanges
- security-based swap data repositories
- security-based swap dealers
- transfer agents

Covered Entities

"Covered Entities" subject to additional requirements include:

- broker-dealers that
    1. maintain custody of securities and cash for customers;
    2. introducing brokers;
    3. have regulatory capital equal to or exceeding $50 million;
    4. have total assets equal to or exceeding $1 billion;
    5. operate as market-makers; or
    6. operate as an operate as an alternative trading system
- clearing agencies
- major security-based swap participants
- Municipal Securities Rulemaking Board
- national securities associations
- national securities exchanges
- security-based swap data repositories
- security-based swap dealers
- transfer agents

Policies and Procedures

The proposed Rule 10 would require all Market Entities to establish, maintain, and enforce written policies and procedures reasonably designed to address their cybersecurity risks. Additionally, Market Entities would be required to review and assess their cybersecurity policies and procedures at least on an annual basis. Market entities would need to prepare a record with respect to the annual review.

Covered Entities would be subject to additional requirements in their cybersecurity policies and procedures. Specifically, Covered Entities would be required to address certain specific issues in their cybersecurity risk management policies and procedures, including: (1) periodic risk assessment; (2) user security and access; (3) information protection from unauthorized access or use; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery. Additionally, Covered Entities would be required to prepare a report with respect to their annual review of their cybersecurity risk management policies and procedures in place of the record that is required from all other Market Entities.

Cybersecurity Incident Reporting

All Market Entities would be required to provide a written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude a cyber incident has occurred or is occurring. In addition, Covered Entities, would be required to submit additional and updated information about significant cybersecurity incidents via filing of Part I of proposed Form SCIR with the Commission. The additional information would have to address the entity's efforts to respond to, and recover from, the incident.

Public Disclosure

Covered Entities would be required to publicly disclose summary descriptions of their cybersecurity risks and the significant incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR. Part II of the proposed Form SCIR would be filed with the Commission and posted on the entity's website. Additionally, broker-dealers that maintain custody of securities or cash for customers and introducing broker-dealers would need to provide the form to customers at the time a customer opens an account, when information is updated, and annually.

Books and Records Requirements

All Market Entities would be required to preserve books and records related to proposed Rule 10.

COMMENTS

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

REQUIRING BOARD OVERSIGHT AND APPROVAL OF A FIRM'S POLICIES AND PROCEDURES IS A NECESSARY ENHANCEMENT.

The Proposal's cybersecurity risk management framework, also known as proposed Rule 10, will enhance the resiliency of our financial markets while also providing Market Entities enough flexibility to tailor their cybersecurity policies and procedures to their unique risks. The Commission's proposed cybersecurity risk management framework is appropriately based on other cybersecurity frameworks established elsewhere in the public sector.[18] The Commission rightly adopts widely accepted definitions established by the National Institute of Standards and Technology and the Cybersecurity and Infrastructure Security Agency for terms in the Proposal, including terms such as "cybersecurity incident," "cybersecurity threat," and "cybersecurity vulnerability." Not only does it make sense to utilize definitions established by government agencies specializing in cybersecurity, but it also fosters continuity across the federal government as to what these terms mean in the cybersecurity field.

Further, the Proposal requires an appropriately comprehensive list of elements to be included in the cybersecurity policies and procedures for Covered Entities, including: periodic risk assessment; user security and access; information protection from unauthorized access or use; cybersecurity threat and vulnerability management; and cybersecurity incident response and recovery.[19] 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, along with certain recordkeeping requirements. Collectively, the Proposal's cybersecurity risk management rules, if followed, will prove critical for Market Entities to better protect themselves from significant cybersecurity incidents in the future.

Although the Commission is wise to draw from other cybersecurity frameworks in fashioning the Proposal, it should firmly 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"[20] 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 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 in other contexts should serve as a safe harbor for compliance with this Proposal.

---

18 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).

19 *See* Release at 20,239.

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

Moreover, the Proposal should include an additional oversight mechanism to ensure that Market Entities' cybersecurity policies and procedures are carried out. A key oversight mechanism that is absent from the Proposal, which the Commission should include, is mandatory review and approval by the entity's board of directors. Oversight and approval of a Market Entity's cybersecurity policies and procedures by the entity's board of directors is critical and consistent with a board of director's responsibilities. Despite this key function normally served by a board of directors, the Proposal largely ignores the role of a board as it relates to the establishment, maintenance, and enforcement of cybersecurity policies and procedures for Market Entities. The Proposal should include a requirement that the board of directors for all Market Entities, or at least Covered Entities, review and approve cybersecurity policies and procedures, review annual reports of any material changes to the policies and procedures, and review proposed Form SCIR reports prior to filing with the Commission. This is a vital oversight mechanism that is lacking in the Proposal and should be included.

According to the Proposal, many broker-dealers reported that cybersecurity policies and procedures "were vetted and approved by senior management and that firms provided annual cybersecurity reports to the board while some also provided ad hoc reports in the event of major cybersecurity events."[21] Due to the rising number of cases of cyberattacks and the rising level of sophistication of the 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 an entity's cybersecurity policies and procedures. The Commission should reject any argument that seeks to insulate a Market Entity's or Covered Entity's board of directors from its duty to oversee adoption and implementation of cybersecurity policies and procedures.

II. THE PROPOSAL'S CYBERSECURITY INCIDENT REPORTING REQUIREMENTS ARE ESSENTIAL FOR MAINTAINING FAIR, ORDERLY, AND EFFICIENT MARKETS, ALTHOUGH THEY SHOULD BE STRENGTHENED IN A NUMBER OF RESPECTS.

The Proposal's cybersecurity incident reporting requirement is an essential component of the Proposal that will enable the Commission, market participants, and investors to better understand the operational, reputational, and financial risks of a cybersecurity attack on a Covered Entity. It will also enable the Commission to better assess potential systemic risks affecting financial markets more broadly. Specifically, the Proposal's requirement for Covered Entities to immediately report significant cybersecurity incidents and keep the Commission updated with subsequent reports will provide the Commission with critical, timely information to evaluate the effects of the incidents on Covered Entities and their counterparties. Additionally, the Proposal's requirement to include relevant summary information regarding their cybersecurity risks and significant incidents on Part II of proposed Form SCIR would provide the Commission and other market participants helpful information about the cyber risks posed by that Covered Entity. Taken together, the Proposal's cybersecurity incident reporting requirements are necessary for the

[21] Release at 20,287 *citing* FINRA, Report on Cybersecurity Practices (Feb. 2015), available at https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf.

Commission to carry out a key component of its tripartite mission: maintaining fair, orderly, and efficient markets.

A. Part I of Proposed Form SCIR Requiring Immediate Incident Reporting by Covered Entities Is an Important Measure, Which Should Be Further Strengthened By Requiring Incident Reporting At Least Within 24 Hours and Through Disclosure of Ransom Demands.

The Commission should require Covered Entities to immediately report significant cybersecurity incidents to the Commission as soon as the Covered Entity has a reasonable basis to conclude that an incident has occurred on Part I of proposed Form SCIR, as proposed.[22] However, the Proposal could be further strengthened by clarifying that incidents must be reported immediately *or within 24 hours*. This clarification will ensure that Covered Entities are reporting significant cybersecurity incidents within a specific time period.[23] 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 against cyberattacks and data breaches. While testifying before Congress, the Director stated in her written testimony that "[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."[24] This is persuasive evidence that the earlier a regulator like the Commission is made aware of a significant cybersecurity incident, the earlier it can analyze the incident and more effectively protect other market participants.

The statement of the Director of CISA is consistent with the purposes and benefits of the Proposal's cybersecurity incident reporting regime. Much in the way that immediate information reporting can help CISA analyze a cybersecurity incident and protect other victims, immediate information reporting from Covered Entities performing critical market services to the Commission will enable the Commission to analyze the incident and protect counterparties to

---

22 Release at 20,248.

23 *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 16,886 (Mar. 9, 2022) (In this comment letter, Better Markets urges the Commission to move to a 24-hour incident reporting timeframe from the proposed 48-hour incident reporting requirement for investment advisers, registered investment companies, and business development companies). By requiring Covered Entities report immediately, or at least within 24 hours of having a reasonable basis to conclude that an incident occurred there is a specific timetable entities would have to comply with. It would have the added benefit of being consistent with Better Markets' recommendation for investment advisers, registered investment companies, and business development companies.

24 *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).

affected Covered Entities or other participants in the market who may also be at risk.[25] Due to the fragmentation of our financial markets and the interconnectedness of participants in those markets, it is critical that the Commission be made aware of significant cybersecurity incidents in real time to ensure the functioning of fair, orderly, and efficient markets.

The Commission should resist any arguments from industry to exclude certain Covered Entities from the immediate notification requirement or to extend the notification period for significant cybersecurity incidents to the Commission by days or weeks. Any delay in requiring the transmittal of this critical information to the Commission will hamper its ability to ensure fair, orderly, and efficient markets.

The Proposal should be further strengthened by requiring Covered Entities to disclose to the Commission on Part I of Form SCIR whether or not any ransom has been paid by the entity, how much has been paid per incident, and in what manner the ransom was paid in (i.e., cash, cryptocurrency, etc.). As proposed, Part I of proposed Form SCIR would not require specific information to be disclosed to the Commission regarding any ransom demanded by the cyber attacker or paid by the Covered Entity.[26] As discussed above and numerous times throughout the Proposal, ransomware attacks are one of the most common types of cyber-attacks companies face today.[27] Collecting this information would give the Commission the ability to identify patterns and threats posed to Covered Entities and financial markets more broadly from ransomware attacks. This information would also aid the Commission in issuing risk alerts to market participants to help prevent ransomware attacks in the future. For those reasons, the Commission should specifically require this information to be provided to the Commission either through a new question added to Part I of proposed Form SCIR related to ransom payments or as part of the information to be included in responses to Question 8 of the form.

B. Part II of Proposed Form SCIR Requiring Disclosure of Cybersecurity Risks and Incidents Is Another Important Reform, Which Should Be Strengthened With Mandatory Disclosures About Chief Information Security Officers and Independent Audits.

The Commission should require Covered Entities to disclose publicly summarized descriptions of their cybersecurity risks and any significant cybersecurity incidents they experienced in the current or previous calendar year in Part II of proposed Form SCIR, as proposed. It is particularly important for introducing broker-dealers and broker-dealers that carry customer accounts to distribute Part II of proposed Form SCIR to prospective and existing customers at the time a customer opens an account, when information is updated, and annually. The information in Part II of proposed Form SCIR will not only provide critical information to the Commission but will also provide critical information to other market participants and investors about the cybersecurity risks and past incidents involving Covered Entities they do business with or allow to hold their funds or securities.

---

25 *See* Release at 20,217.
26 *See* Release at 20,349-20,352.
27 *See* Release at 20,216.

Also as proposed, Part II of proposed Form SCIR should require Covered Entities to include: (1) a summary of cybersecurity risks that could materially benefit its business and operations; and (2) a summary of each significant cybersecurity incident that occurred during the current or previous year. Part II of proposed Form SCIR will inform the Commission, market participants, and investors about the cybersecurity risks and history of past incidents involving Covered Entities. The Proposal points out that cybersecurity incident reporting as proposed in Part II of Form SCIR can assist Commission staff in identifying patterns and trends that pose threats across the industry, information that could enable Covered Entities and other market participants to better protect themselves from cyberattacks and deploy best practices for recovering from them more quickly.[28] Additionally, public disclosure of these risks and past cybersecurity incidents will cut down the "information asymmetry" between Covered Entities and market participants and investors.[29] By any definition, the ability of cyber attackers to disrupt or disable the day-to-day operation of a company or steal proprietary information or client funds is a material risk faced by any company. The disclosures by Covered Entities in Part II of proposed Form SCIR will provide this critical information to the Commission, market participants, and investors, who will benefit from the information as they initially choose financial firms and on an ongoing basis.

The Proposal should be further strengthened by requiring Covered Entities to disclose in Part II of Form SCIR whether or not they employ a designated Chief Information Security Officer ("CISO"). In the Proposal, the Commission considered requiring Covered Entities to designate a CISO as part of their cybersecurity policies and procedures.[30] However, citing the high demand for, and the high costs of employing, a CISO (with a median compensation of $669,903 for companies with revenues of $5 billion or less), the Commission decided against requiring Covered Entities to employ CISOs. While the Commission decided against the approach of requiring Covered Entities to employ a CISO, the Commission should at least require Covered Entities to include a disclosure in Part II of proposed Form SCIR stating whether or not they employ a designated CISO. Despite the cost to employ them, the Commission found that "[a]pproximately two-thirds of the broker-dealers (68%) examined in a 2015 survey had an individual explicitly assigned as the firm's CISO."[31] Thus, while many firms employ CISOs, many do not, and this transparency measure will help investors and others differentiate firms on this basis. It would be especially informative for market participants seeking to do business with a Covered Entity, and prospective and existing investors that may keep funds or securities with Covered Entities, to know whether or not that company has a dedicated CISO on staff.

Additionally, the Proposal should be further strengthened by requiring a simple disclosure in Part II of Form SCIR stating whether or not a Covered Entity's cybersecurity risk management policies and procedures have been audited by an independent third party. Again, the Commission contemplated requiring third-party audits of a Covered Entity's internal controls regarding their

28 Release at 20,305.
29 Release at 20,308.
30 Release at 20,321.
31 Release at 20,287.

cybersecurity policies and procedures.[32] And again, the Commission cited the high costs of such a requirement and did not include it in the Proposal. While the Commission decided against this approach, requiring a disclosure on Part II of proposed Form SCIR stating whether or not a Covered Entity's cybersecurity policies and procedures are audited by an independent, qualified third party would be beneficial to market participants and investors. The Commission rightfully understood that requiring "certification by industry-approved third parties could lead to more robust cybersecurity practices."[33] This specific disclosure would help inform market participants seeking to do business with a Covered Entity, and prospective and existing investors that may keep funds or securities with a Covered Entity, of the robustness of a Covered Entity's cybersecurity policies and procedures.

III. THE PROPOSAL IS ONE IN A SET OF PROPOSALS BY THE COMMISSION TO UPGRADE THE RESILIENCY OF OUR FINANCIAL MARKETS AND VULNERABILITIES DUE TO CYBERSECURITY RISKS, AND THE ENTIRE FRAMEWORK MUST BE ROBUST.

The Proposal represents a necessary but insufficient 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 already proposed rules that will establish a cybersecurity framework and incident reporting regime for investment advisors;[34] extend Reg SCI to more market participants;[35] require uniform cybersecurity disclosure by publicly traded companies;[36] and establish new cybersecurity rules to modernize Reg S-P.[37] These actions, taken together, will help knit together a more resilient cybersecurity framework across our financial markets that better protects investors, advances financial stability, and instills confidence in our markets, both domestically and internationally.

As the Commission considers relevant commentors' views and suggestions, it is important for the Commission to bear in mind that this Proposal is just one in a set of important proposals published for notice-and-comment regarding cybersecurity in our financial markets. In fact, the Commission has already shown its awareness of the inter-related nature of these pending proposals by reopening for comment its proposal on establishing a cybersecurity framework and incident reporting regime for investment advisers, registered investment companies, and business development companies for commentors, a step taken in light of this Proposal. As it proceeds to finalize this Proposal and the others, the Commission should ensure that they all are equally robust so that the resulting overall framework has no weak spots or loopholes that could create

---

32 Release at 20,320.
33 Release at 20,320.
34 Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 16,886 (Mar. 9, 2022).
35 Regulation Systems Compliance and Integrity, 88 Fed. Reg. 23,146 (Apr. 14, 2023).
36 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590 (Mar. 23, 2022).
37 Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 88 Fed. Reg. 20,212 (Apr. 6, 2023).

vulnerabilities to cyberattacks. This holistic approach is necessary to create a more resilient cybersecurity framework across our financial markets.

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

shall@bettermrkets.org
sfarnin@bettermarkets.org

http://www.bettermarkets.org