June 13, 2023

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

Re: Regulation Systems Compliance and Integrity (File No. S7-07-23, RIN 3235-AN25); 88 Fed. Reg. 23146 (Apr. 14, 2023)

Dear Ms. Countryman:

Better Markets[1] appreciates the opportunity to comment on the above-captioned Proposed Rule ("Proposal" or "Release")[2] amending Regulation Systems Compliance and Integrity ("Regulation SCI") to ensure that the technology infrastructure of the U.S. securities markets remains robust, resilient, and secure. The Proposal is an essential step to expand Regulation SCI's application to a broader range of key market participants and to update its provisions to account for the evolution in technology and trading that has occurred since Regulation SCI's adoption in 2014. Once final, the Proposal will benefit investors by requiring that key market participants take the steps necessary to protect their most important systems.

Although these reforms may seem technical or mundane, they are in fact exceedingly important given the increasing dependence of the U.S. securities markets on technology. That dependence increases the risk that failures or even glitches in the systems of key market participants will cause investors significant harm. The growing interconnectedness of key market participants also means that disruptions in the systems of one market participant can have cascading effects across the securities markets and the financial system as a whole.

For these reasons, we support the Proposal, although as detailed below we urge the Commission to strengthen it in some important respects. Specifically, the Commission should

---

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. 23,146 (Apr. 14, 2023).

extend Regulation SCI to more entities than the Proposal contemplates. The Commission should also enhance the reviews that Regulation SCI requires entities to conduct.

Currently, Regulation SCI applies to self-regulatory organizations ("SROs"), alternative trading systems ("ATSs") meeting certain volume thresholds with respect to national market system ("NMS") stocks and non-NMS stocks, exclusive disseminators of consolidated market data, certain competing consolidators of consolidated market data, and certain exempt clearing agencies (collectively, "SCI entities").[3] Regulation SCI governs the obligations of SCI entities with respect to their "SCI systems." "SCI systems" are the technology systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly supports one of six market functions: (1) trading; (2) clearance and settlement; (3) order routing; (4) market data; (5) market regulation; and (6) market surveillance. Regulation SCI requires SCI entities to (1) have policies and procedures in place to help ensure the robustness and resiliency of their SCI systems, and (2) provide notices and reports to the Commission and other market participants of disruptions or other events impacting their systems to facilitate Commission oversight of securities market infrastructure.

The Proposal would amend Regulation SCI to apply it to a broader range of entities and update certain provisions to account for the heightened cybersecurity risks, wider use of cloud service providers, and increasingly interconnected nature of market participants' systems in today's securities markets. Specifically, the Proposal would expand the definition of SCI entities to include registered securities-based swap data repositories ("SBSDRs"), registered broker-dealers exceeding a size threshold, and additional clearing agencies exempt from registration. The Proposal would also require that SCI entities develop and maintain a written inventory of their systems and their classification as SCI systems; require that SCI entities undertake a risk-based assessment of the criticality of each of its third-party service providers; enhance the cybersecurity provisions of Regulation SCI to help ensure that the SCI systems of the most important entities in the securities markets remain secure; revise the requirements applicable to the reviews that SCI entities must conduct of their SCI systems and the reports that they must prepare of those reviews; and require that an SCI entity's policies and procedures identify the current SCI industry standard with which each such policy and procedure is consistent.

The Proposal is a necessary measure to ensure the robustness, resiliency, and security of the technology infrastructure of the U.S. securities markets in an evolving world. Regulation SCI currently applies to entities that play a significant role in the U.S. securities markets and/or have the potential to impact investors, the overall market, or the trading of individual securities in the event of a systems issue. The addition of SBSDRs, certain registered broker-dealers, and additional clearing agencies to the list of SCI entities subject to Regulation SCI acknowledges the important role of these entities in today's securities markets. Nonetheless, the Proposal does not

[3] Registered clearing agencies are SCI entities under Regulation SCI's definition of an SRO.

go far enough in adding certain market participants to the list of SCI entities. The Commission should add to the list of SCI entities ATSs and broker-dealers with significant transaction activity in corporate debt or municipal securities. The Commission should also require that the annual review SCI entities must conduct of their systems be performed by an independent third party, and it should further require that senior management must vouch for the review through certifications.

BACKGROUND

Cyber risk, defined as the risk of loss from dependence on computer systems and digital technologies, continues to grow in the financial system.[4] The interconnectedness of market participants and their systems means that vulnerabilities or flaws in one area of the financial markets can reverberate and cause damage throughout the financial system as a whole.[5] Although cyberattacks are one key threat, technological failures and other malfunctions in computerized systems are just as harmful and must be minimized through appropriate safeguards.

Recent problems demonstrate the need to ensure the resiliency of market infrastructure:

- In March 2023, some Robinhood customers found that their balances had plunged to $0 or even into negative territory due to a malfunction with the company's app. Other customers saw positive balances that were incorrect. Earlier in the month, the app had incorrectly posted that AMC Entertainment had filed for bankruptcy.[6]

- In January 2023, the New York Stock Exchange had a malfunction that led to wild price swings in over 250 stocks, including shares of large companies such as Wells Fargo, Verizon, and Nike. The turmoil resulted from a malfunction in a system at market open. Typically, the NYSE holds an opening auction at the start of the trading day, and those auctions did not occur for the affected stocks. The price swings, which added or eliminated billions of dollars of market value, led the exchange to halt trading in over 80 different shares. Some investors paid way more than the prevailing market price to buy shares, and some paid much less. Other

---

4 Danny Brando, et al., *Implications of Cyber Risk for Financial Stability*, FEDS Notes, Board of Governors of the Federal Reserve System (May 12, 2022), https://doi.org/10.17016/2380-7172.3077https://www federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512 html.

5 Tobias Adrian and Caio Ferreira, *Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards*, International Monetary Fund (Mar. 2, 2023), https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards.

6 Caitlin McCabe, *Robinhood Glitch Briefly Shows Some Traders' Balances at $0 or Less*, Wall Street Journal (May 16, 2023), https://www.wsj.com/livecoverage/stock-market-today-dow-jones-05-16-2023/card/robinhood-glitch-briefly-shows-some-traders-balances-at-0-or-less-0gnaxJQjy6NakvXTKq06?reflink=e2twmkts.

investors had their trades not executed, with significantly reduced trading volume. The NYSE subsequently said that some trades in the 250 stocks would be reversed.[7]

- In November 2022, India's online government bond trading platform experienced malfunctions, which led to users being unable to log in to the system. The problem involved the online platform that provided clearing and settlement services for securities transactions in India. The issue impacted trading volumes that day.[8]

- In September 2020, the Tokyo Stock Exchange experienced an issue that led it to shut down trading for an entire day. The malfunction stemmed from a problem in the hardware that powers the exchange, and the system failed to switch to a backup in response to the problem. The shutdown left investors unable to place orders.[9]

- In August 2020, Robinhood, Vanguard, Schwab, E-Trade, and TD Ameritrade all experienced malfunctions on one day. The trading day was expected to be busy as retail investors wanted to buy shares of Apple and Tesla after stock splits at those companies. The issue affected thousands of customers across the platforms.[10]

The risks that result from the financial markets' dependence on technology will only continue to grow. The financial markets' increasing reliance on technology and the increasing ability of individuals to work from home following the COVID-19 pandemic mean that market participants' technological systems bear more weight than ever before. In this time of transformation, the need to ensure the resiliency of those systems is essential.[11]

OVERVIEW OF THE PROPOSAL

The Commission has proposed amendments to Regulation SCI to ensure that the technology infrastructure of the U.S. securities markets remains robust, resilient, and secure. The first part of the Proposal would extend Regulation SCI to additional entities. Specifically, it would add to the list of SCI entities SBSDRs, registered broker-dealers exceeding a size threshold, and additional clearing agencies exempt from registration. The Proposal notes that these entities play

---

7 Joe Rennison, *N.Y.S.E. Glitch Leads to Wild Swings in Share Prices*, N.Y. Times (Jan. 24, 2023), https://www.nytimes.com/2023/01/24/business/nyse-trading-glitch.html.

8 Bhakti Tambe, *India's online bond trading platform faces technical glitches*, Reuters (Nov. 22, 2022), https://www.nasdaq.com/articles/indias-online-bond-trading-platform-faces-technical-glitches-traders.

9 Ben Dooley, *Tokyo Stock Market Halts Trading for a Day, Citing Glitch*, N.Y. Times (Sept. 30, 2020), https://www.nytimes.com/2020/09/30/business/tokyo-stock-market-glitch html.

10 Alexis Benveniste, *Robinhood, Vanguard and E-Trade report glitches on huge trading day*, CNN (Aug. 31, 2020), https://www.cnn.com/2020/08/31/business/robinhood-app-issues-stock-split/index.html.

11 Tim Maurer and Arthur Nelson, *The Global Cyber Threat*, International Monetary Fund (2021), https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer htm.

a significant role in the U.S. securities markets and/or have the potential to impact investors, the overall market, or the trading of individual securities in the event of a systems issue.

The second part of the Proposal would strengthen the obligations for all SCI entities. This part of the Proposal has five main components:

- The Proposal would require each SCI entity to include in its policies and procedures a written inventory and classification of all of its SCI systems and a program with respect to the lifecycle management of such systems, including the acquisition, integration, support, refresh, and disposal of such systems.

- The Proposal would require that every SCI entity undertake a risk-based assessment of the criticality of each of its third-party providers, including analyses of third-party provider concentration; of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired; and of any security, including cybersecurity, risks posed.

- The Proposal would require that SCI entities include in their policies and procedures a program to prevent unauthorized access to their SCI systems and the information residing therein; conduct penetration testing annually; and monitor and report on a wider range of events classified as systems intrusions.

- The Proposal would require that the annual review that SCI entities must conduct of their systems must be performed by objective personnel having the appropriate experience to conduct reviews of SCI systems; must follow established and documented procedures and standards and use appropriate risk management methodology; must assess risks related to capacity, integrity, resiliency, availability, and security; must assess internal control design and operating effectiveness; and must assess third-party provider management risks and controls.

- The Proposal would require that SCI entities that choose to demonstrate the reasonableness of their policies and procedures under Regulation SCI by identifying them as consistent with current SCI industry standards must identify the SCI industry standard with which each policy and procedure is consistent.

COMMENTS

I. The Commission should add SBSDRs, registered broker-dealers exceeding a size threshold, and additional clearing agencies exempt from registration to the list of SCI entities, and should also add other entities to the list of SCI entities.

A. The Commission should, as proposed, add to the list of SCI entities SBSDRs, registered broker-dealers exceeding a size threshold, and additional clearing agencies.

When the Commission adopted Regulation SCI in 2014, it acknowledged that entities other than those defined as SCI entities could pose risks to the market given their increasing size and importance.[12] The critical role that SBSDRs, large broker-dealers, and exempt clearing agencies play in the securities markets has only increased since the initial adoption of Regulation SCI. As a result, the Commission should add those entities to the list of SCI entities as proposed.

The Commission recognized the importance of SBSDRs, large broker-dealers, and exempt clearing agencies when it first proposed Regulation SCI in 2013. The Commission solicited comment on the inclusion of SBSDRs as SCI entities and conceded the important role SBSDRs play in limiting systemic risk and promoting the stability of the security-based swaps (SBS) market.[13] The Commission similarly solicited comment on the possible inclusion of broker-dealers other than broker-dealers that qualified as significant volume ATSs as SCI entities.[14] In doing so, it acknowledged that some broker-dealers had grown in size and importance to the market in recent years, that recent events had highlighted the significance of systems integrity at large broker-dealers, and that a systems issue at such broker-dealers could pose a significant risk to the market.[15] And the Commission also solicited comment on whether all exempt clearing agencies should be subject to Regulation SCI.[16] Some commentators supported the inclusion of SBSDRs, large broker-dealers, and additional exempt clearing agencies as SCI entities, but the Commission determined not to include them as SCI entities when it first adopted Regulation SCI.[17] The Commission should not delay subjecting them to the requirements of Regulation SCI any longer.

With respect to SBSDRs, an uninterrupted flow of complete, accurate, and timely data reporting is necessary to provide regulators and market participants visibility into the risks faced by major financial institutions in the SBS market; to assess any impact of shocks on markets and firms transacting in SBSs, and to help increase market transparency and promote price discovery. As a result, the infrastructure that facilitates swap data reporting promotes the vibrancy and health

---

12 Release at 23,153.
13 *Id.* at 23,153.
14 *Id.* at 23,157.
15 *Regulation Systems Compliance and Integrity*, 78 Fed. Reg. 18,084, 18,138 & n.334 (Mar. 25, 2013).
16 *Id.* at 18,098.
17 *Regulation Systems Compliance and Integrity*, 79 Fed. Reg. 72252, 72,271, 72,363-72,366 (Dec. 5, 2014).

of the swaps markets and is a linchpin for the functioning of the modern financial system.[18] This means that it is essential to have standards for the technology that enables the use of swap reporting data.[19] As the Commission recognizes, because SBSDRs rely on automated systems and are designed to limit systemic risk and promote the stability of the markets that they serve, including SBSDRs in the definition of SCI entities would better ensure that SBSDR systems are robust, resilient, and secure. Including SBSDRs as SCI entities is also consistent with the inclusion as SCI entities of other entities that play a key price transparency role in their respective markets.[20]

Large broker-dealers should be subject to Regulation SCI for similar reasons. The scale and speed at which large broker-dealers acquire new retail investors, execute huge volumes of transactions in fractions of a second, and influence the markets heightens the risk that these broker-dealers pose. The rising popularity and influence of fintech brokerages only exacerbate these risks. The application of Regulation SCI to large broker-dealers would require them to undertake measures that minimize the frequency and severity of platform failures. As a result, the Commission must expand Regulation SCI to capture broker-dealers that exert a commensurately large influence on the market.[21]

The Commission must also expand Regulation SCI to capture all exempt clearing agencies.[22] As the Commission recognizes, the technological systems that underpin exempt clearing agencies are critical to global financial markets. All exempt clearing agencies offer services that centralize a variety of technological functions. These technological functions help improve the efficiency of the clearance and settlement process by, for example, standardizing and automating functions necessary to complete clearance and settlement. The services that exempt clearing agencies provide have become increasingly reliant on the provision of new technologies to market participants. And over time, the increasing availability of, and access to, such technologies has also increased the dependence that market participants have on such services. This raises the potential that such services could become single points of failure for market participants.[23] Given the important role of exempt clearing agencies in helping to ensure the functioning, stability, and resilience of the securities markets, and their growing technological innovations and interconnectedness, Regulation SCI must apply to all exempt clearing agencies.[24]

---

18 Richard B. Berner, et al., *The Data Reporting Challenge: U.S. Swap Data Reporting and Financial Market Infrastructure* (Feb. 19, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3541248, at 4.

19 *Id.* at 27.

20 Release at 23,154.

21 Ya Sheng Lin, Note, *Why Robinhood is not a Fiduciary*, 39 YALE J. ON REG. 1445, 1483-85 (2022).

22 The fact that some clearing agencies are exempt from registration requirements is irrelevant to the need to subject them to the requirements that Regulation SCI imposes on key market participants, as exempt clearing agencies make available to buyers and sellers of securities an increasingly wide array of technology services that help centralize and automate the clearance and settlement of securities transactions. Release at 23,171.

23 Release at 23,170.

24 *Id.* at 23,171.

B. The Commission should add to the list of SCI entities ATSs and broker-dealers with significant transaction activity in corporate debt or municipal securities.

When it first proposed Regulation SCI in 2013, the Commission proposed including as SCI entities ATSs trading corporate debt or municipal securities that exceeded five percent or more of either average daily dollar volume or average daily transaction volume traded in the United States. However, the Commission did not adopt that proposal. The Commission determined that, because at that time the corporate debt and municipal securities markets relied less heavily on automation and electronic trading than did markets that traded NMS stocks or equity securities that were not NMS stocks, Regulation SCI did not need to apply to the fixed-income markets.[25]

As the Commission now recognizes, the gap in electronic trading between equity and fixed-income markets has diminished considerably in recent years. The last decade has seen an explosion of new technologies in what was once an overwhelmingly manual market. The COVID-19 pandemic intensified the trend, driving an unprecedented adoption of electronification and automation in fixed-income trading. Some estimate that electronic trading of corporate bonds has grown from around 15-20% in 2015 to close to 30% in 2022, with the potential to continue to grow as high as 60-70% over the next five to ten years.[26] Almost half of all government bond trading is already electronic and is expected to jump to two-thirds in the near future.[27]

As a result, the Commission should now extend Regulation SCI to ATSs and broker-dealers trading corporate debt or municipal securities that exceed five percent or more of either average daily dollar volume or average daily transaction volume traded in the United States.[28] Extending Regulation SCI to these ATSs and broker-dealers responds to the growing dependence on critical electronic trading infrastructures in the fixed-income markets.[29] It also responds to the fact that the electronic trading infrastructures in the fixed-income markets have developed into a critical part of the financial ecosystem and could pose broader risks in the event of a failure. For example, a dislocation on an automated trading platform or system in the fixed-income markets could quickly spill over into other markets. As a result, firms must develop and maintain appropriate risk management systems.[30] Applying Regulation SCI to firms with significant transaction activity in corporate debt or municipal securities would ensure that they do so.

---

25 *Id*. at 23,172-23,173.

26 Dan Romanelli, *Growth, automation, and regulation—why 2022 is a pivotal year for fixed income trading*, The Trade (Aug. 16, 2022), https://www.thetradenews.com/growth-automation-and-regulation-why-2022-is-a-pivotal-year-for-fixed-income-trading/.

27 Robin Wigglesworth, *Bond trading finally dragged into the digital age*, Financial Times (Feb. 22, 2021), https://www.ft.com/content/683effc4-993a-4baf-bc17-8ba70b96c06a.

28 The five percent threshold mirrors other sized-based thresholds in Regulation SCI.

29 *Electronic Trading in Fixed Income Markets* 2, Bank for International Settlements (Jan. 2016), https://www.bis.org/publ/mktc07.pdf.

30 Bank for International Settlements, supra note 29, at 27-28.

II. The Commission should enhance the requirements applicable to all SCI entities by strengthening their obligations to oversee third-party providers, their obligations to have cybersecurity measures, and their obligations to review their systems.

A. The Commission should, as proposed, require SCI entities to have a third-party provider management program, to have a program to prevent unauthorized access to their SCI systems that includes conducting penetrating testing annually, and to notify the Commission of events that disrupt their systems and unsuccessful but significant attempts to enter their SCI systems.

When the Commission adopted Regulation SCI in 2014, it recognized that an SCI entity might choose to use third parties to assist it in running its SCI systems.[31] The use of third-party providers offers advantages to SCI entities due to the benefits they deliver when employed appropriately. Nonetheless, the use of third-party providers also carries risks—an SCI entity's systems could be negatively impacted if a third-party provider's systems are compromised or if a third-party provider's services experience a disruption or shutdown.[32] Currently, Regulation SCI requires only that an SCI entity is responsible for ensuring that it is able to satisfy the requirements of Regulation SCI for systems operated on behalf of the SCI entity by a third party.[33] As the Commission recognizes, this standard is no longer sufficient in light of the proliferation of the use and influence of third-party providers since the adoption of Regulation SCI.

There is no question that financial institutions have increased their use of third-party service providers in recent years.[34] The COVID-19 pandemic accelerated this preexisting trend.[35] Financial institutions' increasing reliance on third-party service providers magnifies the risks that they pose.[36] The more a financial institution contracts with a third-party service provider, the more exposed the financial institution is to the risk that the provider will be unable to perform as intended.[37] Additional risks result from the fact that third-party service providers may in turn subcontract some services.[38] The risks also increase as large service providers gain market share and some service providers become more specialized.[39] This is of particular concern where many institutions rely on the same third-party provider for key services.[40] When technology innovations rely on relatively few companies to provide supporting infrastructure, the risk grows that financial or operational failures or faults at the companies providing that infrastructure could disrupt the activities of multiple financial institutions or financial markets.[41] Accordingly, the increasing use

---

31 Release at 23,176.
32 *Id.*
33 *Id.*
34 FINANCIAL STABILITY OVERSIGHT COUNSEL, 2021 ANNUAL REPORT 125 (2021), https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf (hereinafter "FSOC REPORT").
35 *Id.*
36 *Id.* at 16.
37 *Id.* at 174.
38 *Id.* at 125.
39 *Id.*
40 *Id.*
41 *Id.* at 174.

of third-party service providers by financial institutions threatens the operational risk mitigation capabilities not just at individual institutions but also of the financial sector as a whole.[42]

As a result, the Commission correctly recognizes that with the continued and increasing use of third-party providers by SCI entities and, in some cases, with third-party providers playing increasingly important and even critical roles in ensuring the reliable, resilient, and secure operations of SCI systems, it is appropriate to strengthen Regulation SCI's requirements with respect to SCI entities' use of third-party providers and the management of such relationships.[43] Specifically, it is appropriate to require that every SCI entity undertake a risk-based assessment of the criticality of each of its third-party providers, including analyses of third-party provider concentration; of key dependencies if the third-party provider's functionality, support, or service were to become unavailable or materially impaired; and of any security, including cybersecurity, risks posed. These measures respond to the increasing use and importance of third-party providers and the concomitant need for SCI entities to better oversee those relationships.[44]

The increasing threat of cybersecurity attacks since the adoption of Regulation SCI in 2014 means that the Commission should also adopt the proposed enhancements to Regulation SCI to require SCI entities to have a program that addresses cybersecurity specifically. Indeed, surveys consistently rank cyberattacks as among the top risks to financial stability.[45] And the basic task of cybersecurity is to ensure that those, and only those, authorized to access data or computer systems are allowed to do so.[46] Yet, currently, Regulation SCI does not specify the need for an SCI entity to have access controls designed to protect both the security of its systems and the information residing therein; it requires only that SCI entities have levels of security adequate to maintain operational capabilities.[47] The Proposal addresses this flaw by requiring that SCI entities have a program to limit access to SCI systems to authorized purposes and uses.[48]

The prevalence of cybersecurity attacks in recent years further supports the proposed revision to the time period for penetration testing. When the Commission adopted Regulation SCI in 2014, it required penetration testing only once every three years. But now, most institutions

---

42 *Id.* at 16.

43 Release at 23,176; *see also* FSOC REPORT, supra note 34, at 125 (recognizing that "financial institutions that contract with a third-party service provider may expose themselves to additional risks if the third party is not appropriately managed when performing services on behalf of the financial institution").

44 *See* FSOC REPORT, supra note 34, at 125 ("Financial institutions are expected to appropriately manage and evaluate the risks associated with each third-party relationship, as engaging a third party to perform functions does not relieve a financial institution of its own legal and regulatory obligations. Financial institutions should conduct appropriate due diligence before entering into a third-party relationship and exercise effective oversight and management throughout the life of the relationship.").

45 Thomas E. Eisenbach, et al., *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, at 1, Federal Reserve Bank of New York (2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf?sc_lang=en.

46 Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1501 (2017).

47 Release at 23,182-23,183.

48 *Id.* at 23,183.

consider annual penetration testing common practice.[49] As the Commission recognizes, more frequent testing would help to ensure that robust measures are in place to protect an SCI entity's systems from cybersecurity events.[50] Accordingly, the Commission should now require that SCI entities conduct penetration testing annually as contemplated in the Proposal.

The Commission should further adopt the proposed expansion of the types of events that SCI entities must report to the Commission. Regulation SCI requires notification to the Commission of systems intrusions, which it currently defines as any unauthorized entry into the SCI entity's SCI systems. The Proposal would expand the definition of systems intrusions to also include cybersecurity events that disrupt, or significantly degrade, the normal operations of an SCI system. It would also expand the definition to include significant attempted unauthorized entries into the SCI systems of an SCI entity. Notification of these events would provide the Commission with more complete information to assess the security status of an SCI entity.[51]

Although some may say that the requirement to report unsuccessful attempts to enter an SCI entity's SCI systems is unnecessary,[52] the Commission should resist pressure to eliminate this requirement. Information about threats that are thwarted furthers the development of cybersecurity best practices.[53] Indeed, an analysis of unsuccessful but significant unauthorized access attempts is critically important to the ongoing development and improvement of cybersecurity programs.[54] Notice of such threats facilitates both information sharing about serious events that threaten an institution's integrity and the ability to oversee threats to the markets as a whole.[55] Notification would ensure that the Commission is made aware when an SCI entity is the subject of a significant cybersecurity threat, and would provide important information regarding threats that may be posed to other entities.[56] As a result, the Commission should adopt this part of the Proposal.[57]

---

49 Emily E. Bayyard, Note and Comment, *The Rise of Cybercrime and the Need for State Cybersecurity Regulations*, 45 RUTGERS COMPUTER AND TECH. L.J. 69, 93 (2019).

50 Release at 23,183.

51 *Id.* at 23,184-23,185.

52 *See, e.g.*, Microsoft, Comment Letter on Proposed SEC Cybersecurity Rules at 3 (June 5, 2023), https://www.sec.gov/comments/s7-07-23/s70723-199880-399982.pdf.

53 Ernest Edward Badway and Christie McGuiness, *The Criminal, Regulatory, and Civil Issues Surrounding Intellectual Property and Cybersecurity*, 14 BROOK. J. CORP. FIN. & COM. L. 181, 224-25 (2020) ("The risks and costs associated with even an attempted cyber-attack are great even if no customer or employee information is compromised. . . . When companies report on their cyber-controls, vulnerabilities, and defenses, they are more prone to take cybersecurity seriously. This incentivizes improved cyber-measures that better secure customer information.").

54 *Frequently Asked Questions Regarding 23 NYCRR Part 500*, N.Y. STATE DEP'T OF FIN. SERVS. (Mar. 23, 2018), https://perma.cc/4CDY-3SQ4.

55 *Id.*

56 Release at 23,184.

57 *Cf. Frequently Asked Questions (FAQs) Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information Through Suspicious Activity Reports (SARs)*, FIN. CRIMES ENF'T NETWORK (Oct. 25, 2016), https://perma.cc/T5DQ-KLHZ (providing that an "otherwise reportable cyber-event should be reported regardless of whether it is considered unsuccessful").

B. The Commission should require that the annual review SCI entities must conduct of their systems be performed by an independent third party, and that senior management must vouch for the review through certifications.

Regulation SCI requires that SCI entities conduct a review of their compliance with Regulation SCI annually. Currently, Regulation SCI requires that the review be performed by objective but not necessarily independent personnel having appropriate experience to conduct reviews of SCI systems and must contain a risk assessment with respect to the SCI systems of the SCI entity and an assessment of the internal control design and effectiveness of the SCI entity's SCI systems. Regulation SCI requires SCI entities to submit a report of the SCI review to the senior management of the SCI entity for review and to submit to the Commission and the board of directors of the SCI entity a report of the SCI review together with any response by senior management.

Although the Proposal improves upon the current requirements for the SCI compliance review by making a response by senior management to the report of the SCI review mandatory rather than permissive, the Proposal does not go far enough. First, the Commission should ensure compliance and accountability by requiring senior officer certifications. Such certifications are an important regulatory tool, recognized by Section 302 of the Sarbanes-Oxley Act of 2022 specifically, which promotes corporate accountability by requiring that issuers' periodic financial reports include certifications from the issuers' Chief Executive Officers and Chief Financial Officers. Regulation SCI should include a similar requirement. It is not enough that senior management be required to respond to reports of the SCI compliance review. Rather, senior management must be required to vouch for the report through certifications that, at a minimum, set forth the official's name and position and attest to the accuracy and reliability of the report.[58]

Second, the Commission should require that the annual SCI compliance review be conducted by an independent third party. The Proposal states that the Commission continues to believe that the requirement that the review be conducted by "objective personnel," which may include personnel at the SCI entity, is appropriate.[59] But the Commission does not explain how a review conducted by personnel at the SCI entity could be objective. All individuals at the SCI entity, whether they be considered "objective" or not, have a presumptive conflict of interest with respect to evaluating compliance given their duty of loyalty to the entity and their desire to protect

---

[58] Better Markets, Comment Letter on Regulation Systems Compliance and Integrity at 6 (July 8, 2013), https://bettermarkets.org/sites/default/files/documents/SEC-%20CL-%20Systems%20Compliance%20and%20Integrity-%207-8-13.pdf. The precise wording of the certification could mirror Section 302 of Sarbanes-Oxley, substituting language referring to "internal controls" with the phrase "systems compliance and integrity." *Id.*; *see also* Pub. L. No. 107-204, 116 Stat. 745, 777 (July 30, 2002), https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf.

[59] Release at 23,187.

their employment status. A mandatory review by an independent third party would provide the necessary degree of independence to ensure a reliable and comprehensive review.[60]

III. The Commission should adopt the proposed amendments to Regulation SCI regardless of the fact that SCI entities would also be required to comply with other rules in other Commission proposals to address cybersecurity risks.

In addition to the Proposal, the Commission has also proposed amendments to Regulation S-P ("the Regulation S-P Proposal") as well as new rules addressing cybersecurity specifically ("the Exchange Act Cybersecurity Proposal"). The Proposal recognizes that the Regulation S-P Proposal and the Exchange Act Cybersecurity Proposal would require that certain SCI entities have policies and procedures that address certain types of cybersecurity risks. But the Proposal has a different purpose and scope than either the Regulation S-P Proposal or the Exchange Act Cybersecurity Proposal and therefore should be adopted regardless of any overlap.

Regulation S-P currently requires brokers, dealers, investment companies, and registered investment advisers to adopt written policies and procedures to ensure that administrative, technical, and physical safeguards are in place to protect customer records and information ("the safeguards rule"). Regulation S-P also currently requires brokers, dealers, investment companies, and registered investment advisers, as well as transfer agents registered with the Commission, to properly dispose of consumer report information ("the disposal rule"). The Regulation S-P proposal would amend the scope of information covered by the safeguards rule and the disposal rule, but it would not fundamentally broaden the scope of the provisions. Therefore, the requirements of Regulation S-P that pertain to cybersecurity would continue to apply to customer and consumer-related information. The cybersecurity requirements of Regulation S-P would not apply to other types of information stored on the information systems of the covered entities.[61]

As discussed above, the Proposal would require that SCI entities include in their policies and procedures a program to prevent unauthorized access to all of their SCI systems and the information therein. The Proposal thus would impose broader requirements on SCI entities than would the Regulation S-P Proposal, which is limited to customer and consumer-related information. As a result, the Commission should adopt the Proposal regardless of whether the Regulation S-P Proposal would also impose cybersecurity requirements on SCI entities.

The Commission should adopt the Proposal regardless of the Exchange Act Cybersecurity Proposal for similar reasons. The Exchange Act Cybersecurity Proposal would require covered entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[62] Again, the provisions of the Proposal apply more

---

60 Better Markets, supra note 58, at 5.
61 Release at 23,193.
62 *Id.* at 23,193-23,194

broadly with respect to SCI entities' SCI systems. For example, the Exchange Act Cybersecurity Proposal would establish minimum cybersecurity rules for all broker-dealers, but it would not independently address weaknesses in broker-dealer operational capacity or resiliency not attributable to cybersecurity breaches.[63] For this reason, the Commission should adopt the Proposal even if it also adopts the Exchange Act Cybersecurity Proposal.

Moreover, any increased costs from compliance with both the Proposal and the other cybersecurity-related proposals would be offset by the benefits of requiring compliance with Regulation SCI. Indeed, many of the processes that Regulation SCI requires—such as the maintenance of infrastructural capacity, resilience against cyberattacks, and remediation procedures—are generally considered sound business practices and have been implemented across firms in the United States. In the long run, compliance with Regulation SCI is likely to reduce costs overall by minimizing the disruptions that result when technological failures occur.[64]

CONCLUSION

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

Sincerely,

Stephen W. Hall
Legal Director and Securities Specialist

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

[redacted]
http://www.bettermarkets.org

63 *Id.* at 23,158 n.145.
64 Lin, supra note 21, at 1486.