JEFFREY S. DAVIS
Senior Vice President,
Senior Deputy General Counsel
805 King Farm Blvd
Rockville, MD 20850

June 2, 2023

Ms. Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F. Street NE.
Washington, DC 20549

Re: Regulation Systems Compliance and Integrity, File No. S7-07-23, Release No. 34-97143;

Cybersecurity Risk Management Rule, File No. S7-06-23, Release No. 34-97142;

Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, File No. S7-05-23, Release No. 34-97141

Dear Ms. Countryman:

The Nasdaq Stock Market LLC[1] ("Nasdaq") appreciates the opportunity to comment on three recent proposals related to cybersecurity that the Securities and Exchange Commission ("Commission" or "SEC") published on March 15, 2023.[2] The Proposals are important because cybersecurity threats pose an ongoing and escalating risk to U.S. securities markets and investors. Requiring various financial institutions and market entities[3] to address these

---

1 The Nasdaq Stock Market LLC is registered as a national securities exchange and is wholly owned by Nasdaq, Inc. References to "Nasdaq" throughout the document are references to The Nasdaq Stock Market LLC when referring to the application of the Proposals to our exchanges but should be construed to be Nasdaq, Inc when referring to Nasdaq more broadly as a global organization.

2 See Securities Exchange Act Release Nos. 97143 (March 15, 2023), 88 FR 23146 (April 14, 2023) (File No. S7-07-23) ("Reg SCI Proposal") ; 97142 (March 15, 2023), 88 FR 20212 (April 5, 2023) (File No. S7-06-23) ("New Rule 10 Proposal"); and 97141 (March 15, 2023), 88 FR 20616 (April 6, 2023) (File No. S7-05-23) ("Reg S-P Proposal") (collectively, the "Proposals").

3 The Proposals address requirements 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, registered investment advisors and transfer agents (collectively, "market entities").

cybersecurity risks through policies and procedures, incident response programs, third-party management, notifications and/or public disclosures can promote transparency and consistency. Investors, issuers and other market participants benefit from healthy capital markets that promote trust and transparency.

While Nasdaq supports the Commissions objectives in enhancing cybersecurity and safeguarding information, the multitude of regulators and regulations addressing these risks, including the current three Proposals and prior proposals by the Commission and other contemplated regulation from other agencies may jeopardize the ability to achieve these objectives.[4] If each proposal were to be adopted, the result would be multiple overlapping and often incompatible obligations on certain market entities and their supply chains. To that end, Nasdaq exhorts the Commission to deliberate and collaborate with other agencies and global regulators on a harmonized approach to optimize the efforts of market entities to protect their information resources and also comply with state and federal cybersecurity regulations. Such harmonization is central to the Biden Administration's National Cybersecurity Strategy of 2023 objective to "Harmonize and Streamline New and Existing Regulation".[5] It is also consistent with the approach taken by the Cybersecurity and Infrastructure Security Agency (CISA) in implementing Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), whose rules will also apply to many entities covered by the Proposals.

Below Nasdaq outlines suggestions to harmonize cybersecurity regulation. Specifically, Nasdaq suggests (1) streamlining the timeframes for reporting cybersecurity incidents; (2) creating a single streamlined cybersecurity notification; and (3) providing for reporting delays for ongoing investigations where public disclosure is required.

I. Harmonize Cybersecurity Regulation

As a technology and financial services company which operates regulated entities in the United States and across the globe , Nasdaq is home to over 5,500 listings worldwide that drive the global economy and provide investment opportunities for investors. As an exchange operator of multiple self-regulatory organizations, and broker-dealers, Nasdaq is committed to protecting investors and the public interest. In these unique roles, Nasdaq has a heightened focus on cybersecurity and its attendant risks.

Nasdaq, like other companies, is also subject to a variety of regulations governing cybersecurity[6] each of which define what constitutes a "cybersecurity incident," the types of

---

4 See Securities Exchange Act Release No. 94382 (March 9, 2022), 87 FR 16590 (March 23, 2022) (File No. S7-05-22) (Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure).

5 See https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

6 Among other reporting requirements, in the United States, as an exchange operator of multiple self-regulatory organizations, Nasdaq is registered with the SEC and is required to report cybersecurity matters to the SEC. The primary SEC regulatory framework

cybersecurity incidents subject to regulation, set timeframes for notification (to regulators, customers and/or affected individuals) and other disclosures, and require governance, policies, procedures, controls and specialized contracting with service providers. Like many other global businesses, Nasdaq is itself a vendor and service provider to customers in regulated industries; as a result, it is also exposed either via contract or direct regulation to regulatory regimes that apply to its customers. While they share the same core objective of protecting systems and data, in some cases, these regulations, vary significantly, creating administrative burdens that divert critical resources away from that core objective. In the event of security incident, where all resources should be focused on addressing the threat at hand, disharmonized regulatory requirements run the risk of negatively impacting response effectiveness as companies focus on addressing varying regulatory requirements.

Nasdaq believes that a harmonized, standards-based approach to cybersecurity regulation among state, federal and global regulators would provide companies with the ability to design robust and cost-effective cybersecurity programs. For that reason, Nasdaq believes that the Commission should, to the greatest extent possible, align new, proposed obligations with existing cybersecurity standards and aim to create a standardized set of obligations across regulatory frameworks that will define the "best practices" for program design.[7] This standardization is most salient for obligations relating to cybersecurity incidents, timeframes for reporting, governance practices, controls and procedures and supplier requirements.

By way of example:

- The reporting deadline for the New Rule 10 Proposal is no later than 48 hours, upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring,[8] while a Reg SCI entity is required to report a cybersecurity matter immediately upon having a reasonable basis to conclude

---

applicable to Nasdaq with respect to cybersecurity is the SEC's Regulation Systems Compliance and Integrity ("Reg SCI"), see 17 CFR Part 242.1000-10007. Nasdaq as a public company is subject to a variety of reporting requirements, which includes cybersecurity reporting. As an operator of broker-dealers, Nasdaq is subject to Privacy of Consumer Financial Information (Regulation S-P), 17 CFR Part 248, Subpart A.

[7] There are a number of industry standards that describe best practices such as, the National Institute of Standards and Technology ("NIST"), the International Organisation for Standardization ("ISO"), the Information Systems Audit and Control Association ("ISACA"), and the Information Technology Infrastructure Library ("ITIL"). Standardized tools are also acknowledged as industry standards or best practices such as, the Financial Services Sector Coordinating Council ("FSSCC") Cybersecurity Profile, the NIST Cybersecurity Framework, the ISO Cybersecurity Standard, and the ISACA COBIT Framework, among others.

[8] See paragraph (c)(2) of proposed Rule 10.

that an SCI Event has occurred, but no later than 24 hours thereafter.[9] In contrast, the New York State Department of Financial Services ("NYDFS") proposed second amendment to address cybersecurity requires that each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred.[10]

- Another example of incongruent obligations is with respect to third-party requirements related to cybersecurity. The Reg SCI proposal requires that a Reg SCI entity have in place policies and procedures to manage and oversee third-party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems.[11] In contrast, the New Rule 10 Proposal requires Covered Entities to have written policies and procedures designed, among other things, to oversee service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems.[12] Further, New Rule 10 requires a Covered Entity to identify its service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and the information residing on those systems, and assess the cybersecurity risks associated with its use of these service providers.[13]
- A final point of comparison concerns the definitions of "cyber incident" and "significant cyber incident." New Rule 10 defines a "cybersecurity incident" to mean an unauthorized occurrence on or conducted through a market entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems.[14] New Rule 10 defines a "significant cybersecurity incident to mean a cybersecurity incident, or a group of related cybersecurity incidents, that: (i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or (ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such

---

9 See 17 CFR 242.1002(b).

10 See proposed amendments to 23 NYCRR 500.

11 See SCI Adopting Release, supra note 1, at 72276.

12 See paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Covered Entities), and paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Entities).

13 See paragraph (b)(1)(i)(A)(*2*) of proposed Rule 10.

14 See paragraph (a)(2) of New Rule 10.

> information or information systems results in or is reasonably likely to result in: (A) Substantial harm to the market entity; or (B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.[15] In contrast, Presidential Directive 41 defines a cyber incident as an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.[16] Presidential Directive 41 defines a significant cyber incident as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.[17]

One such harmonized approach was detailed in a report[18] recently published by the Financial Stability Board ("FSB") with the purpose of achieving greater convergence in cyber incident reporting. The FSB report sets out recommendations to address impediments to achieving greater harmonization, adds terms to create a "common language" necessary for convergence, and identifies common types of information submitted to authorities for cyber incident reporting.[19] The FSB report outlines a common format for incident reporting that promotes consistent reporting but avoids a one-size-fits-all approach.[20] This approach is consistent with the National Cybersecurity Strategy which states:

> Effective regulations minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets. By leveraging existing international standards in a manner consistent with current policy and law, regulatory agencies can minimize the burden of unique requirements and reduce the need for regulatory harmonization.

---

15 See paragraph (a)(10) of New Rule 10.

16 See Presidential Policy Directive – United States Cyber Incident Coordination, PPD-41 (July 26, 2016)

17 Id.

18 See Financial Stability Board's *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting,* April 13, 2023.

19 Id.

20 Id.

> Where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms.

Nasdaq recommends such a harmonized approach include permitting market entities to complete one common cybersecurity reporting form that would meet its reporting requirements for all state and federal regulators. This reporting could then be done through one primary regulatory or central system which would then distribute and coordinate any U.S. government response; we believe this is consistent with the intent behind the passage of CIRCIA.

A. Streamline Timeframes

The Commission should streamline timeframes for reporting cybersecurity incidents and, in determining an appropriate timeframe, consider timeframes required by other state and federal regulators. Each of the Proposals, as well as a prior SEC proposal related to public companies,[21] sets forth different timelines for reporting cybersecurity incidents. The discovery of a potential breach of a market entity's information systems would trigger a series of necessary actions (all done concurrent with what will likely be a crisis response involving many simultaneous moving parts) to arrive at a determination that a breach was significant or resulted in access to or use of sensitive customer information including, but not limited to, an internal investigation, extensive communication with and oversight from senior management, and the board of directors, together with communication with external parties (outside counsel, advisors, expert consultants and regulators). The timeframe must provide the entity with adequate time to investigate and formulate next steps. Requirements that mandate that the entity prepare a fulsome and thorough disclosure may hinder a market entity's investigation into a breach, potentially precluding a deliberate and systematic investigation, which could impair its response and result in incorrect or incomplete conclusions being drawn early on and being disclosed. We believe disclosures that are premature, and potentially incomplete or ultimately misleading, do not further investor protection and do not promote well-functioning orderly and efficient markets. Nasdaq acknowledges that in some cases more expeditious disclosure may be justified and requests the Commission consider providing some flexibility in the timing of the disclosure to allow entities the necessary time to prepare and file more informed public disclosures.

B. *Streamline Notification Requirements*

Regulated market entities should be permitted to comply with various state and federal cybersecurity notification obligations with a single streamlined form. This approach could be a meaningful step in creating a single standardized reporting obligation among different regulators all seeking to address the risks of cybersecurity events. A harmonized cybersecurity regime with standardized cyber incident reporting requirements would avail market entities of the time necessary to focus on their cybersecurity programs. In the event of a cybersecurity incident, it is paramount for a market entity to understand the scope and nature of the cybersecurity incident and immediately commence remediation efforts to limit the amount of damage that such an incident may cause. As noted above, time is of the essence for a market entity dealing with a cybersecurity incident. However, duplicative or unaligned obligations under the Proposals, on

[21] See supra note 4.

the one hand, and other applicable cybersecurity obligations on the other hand, would have the effect of focusing resources away from remediation and towards compliance with the formal requirements of each regime.

A harmonized cybersecurity regime would permit market entities to focus first on protecting the market entity's information systems and avert further damage over other priorities. Of note, the final rule of the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation, titled the Computer-Security Incident Notification Requirements for Banking Organizations and Their Banking Service Providers,[22] noted that it was designed to ensure that the appropriate agency receives timely notice of significant emergent incidents, while providing flexibility to the banking organization to determine the content of the notification. Further, it stated that a limited notification requirement will alert the agencies to such incidents without unduly burdening banking organizations with detailed reporting requirements, especially when certain information may not yet be known to the banking organizations.[23] A similar approach should be considered by the Commission in establishing notification requirements for these Proposals.

C. Allow Law Enforcement and Investigation Delays

The Proposals should provide for reporting delays for ongoing investigations where public disclosure is required. If a potential breach is determined to be significant or resulted in access to or use of sensitive customer information, a market entity would have concomitant obligations to communicate with customers, comply with statutory and/or regulatory obligations, and communicate with law enforcement within potentially the same time period to disclose a cybersecurity incident. The Proposals do not provide for a reporting delay for ongoing investigations where public reporting is required, even when requested by law enforcement and otherwise permitted under state law and other federal laws. Disclosures of cybersecurity incidents may serve to hamper an investigation where the scope of the intrusion may yet be unknown, which may strain collaboration with law enforcement. Worse, the obligation to publicly disclose may reveal additional information to an unauthorized intruder who may still have access to the company's information systems at the time the disclosure is made and potentially further harm the company.[24] The Commission should strongly consider the conflicts raised by public disclosure where an investigation is ongoing.

---

22 See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 FR 66424 (November 23, 2021) (OCC-2020-038).

23 Id. at 66432.

24 In the current threat environment where professionalized hacking and ransomware groups may attack multiple targets at once, law enforcement may have an interest in delaying disclosure to address the full scope of an attack across a group of victims.

II. Reg. SCI Proposal and Associated Cloud Guidance

Nasdaq also wishes to comment specifically on the Reg. SCI Proposal with respect to both the SEC's proposed rule text amendments as well as the SCI imbedded guidance for the use of cloud service providers ("CSPs") to support the operation of regulated systems ("SCI Systems").

As a threshold matter, Nasdaq supports the Commission's principles-based approach to regulating the risks inherent in the use of technology to operate the markets. The Commission designed Regulation SCI to be adaptable, and during the course of its almost 10 year existence, it has been largely successful in keeping pace with the dramatic shifts in market technology that have occurred. We also agree with the Commission that there is room to enhance Reg. SCI, including by broadening its reach so that it applies, not only to incumbent exchanges, but also to other market participants and operators that perform similar functions to exchanges and which are similarly critical to the safe, sound, and orderly functioning of the markets. We also believe that specific guidance and standards would be appropriate to help entities subject to Reg. SCI ("SCI Entities") understand how to approach the adoption of emerging and transformational technologies like cloud, where general principles often fail to suggest an appropriate manner of addressing fundamental design and implementation questions. The absence of clear guidance and standards for the use of the cloud hinders its adoption, and it has significant implications, not only for SCI Entities, whose planning and investments it places at risk, but also for customers, vendors, and most importantly, investors.

First, Nasdaq supports amendments to Reg. SCI that would ensure that like market participants are subject to the same standards — and that investors receive the same protection —for security, integrity, and resiliency, regardless of their regulatory classification as an exchange, an ATS, or a large broker-dealer. As the Commission has said elsewhere, regulatory disparities that exist among the various categories of market participants create an uneven competitive environment; this environment unfairly advantages lesser- relative to more-regulated entities.[25] Especially now that as much as half of daily trading can occur off-exchange on any given day, and that in in the retail markets, approximately 90 percent of trading occurs every day among a handful of large wholesale broker-dealers, [26] the markets and investors depend upon large broker dealers to be secure, operationally sound, and resilient just as they depend upon exchanges to be so. Nasdaq does not opine on the appropriate threshold for subjecting a broker-dealer to Reg. SCI except that it believes that the threshold should be low enough to ensure that it captures all major market participants, but not so low as to create a barrier for new and emerging participants to enter the markets and compete.

---

25 See Securities Exchange Act Release No. 34-96495 (December 14, 2022), 88 FR 128 (January 3, 2023); Securities Exchange Act Release No. 34-96494 (December 14, 2022), 87 FR 80266 (December 29, 2022); Securities Exchange Act Release No. 34-96496 (December 14, 2022), 88 FR 5440 (January 27, 2023); Securities Exchange Act Release No. 34-96493 (December 14, 2022), 88 FR 3786 (January 20, 2023).

26 See Securities Exchange Act Release No. 34-96495 (December 14, 2022), 88 FR 128, at 129 (January 3, 2023).

Second, Nasdaq supports many of the Commission's substantive modifications to Reg. SCI, and in particular, those that pertain to management of third party service provider relationships. The SEC's existing guidance for SCI Entities to utilize service providers to support the operation of SCI Systems is sound and is broadly consistent with vendor management regulations and guidance in other contexts and jurisdictions.[27] Nevertheless, it lacks many of the specifics that these other regimes prescribe, such as requirements for regulated entities to establish formal vendor management programs, to draft written policies and procedures to govern the regulated entity's relationship with its vendors and manage the risks inherent in those relationships, to conduct risk-based assessments of vendors' capabilities, willingness, and reputation for conducting business in a manner that would allow for a regulated entity to continue to satisfy its obligations. [28]

Nasdaq notes that it has long-since incorporated these measures into its own vendor management program. It did so on a voluntarily basis, as a matter of prudence and best practice. We welcome the Commission's proposal to require others to do the same.

Likewise, as noted above, Nasdaq welcomes the Commission's specific guidance on the use of CSPs to support SCI Entities in operating their SCI Systems in the cloud. To date, the Commission has been slow to embrace the use of the cloud for regulated workloads even as many others have done so, including other federal financial regulators, European and Asian securities regulators, [29] and even as the SEC itself. Although the Commission been quiet and cautious on this issue from a regulatory standpoint, we appreciate the fact that it also has been open-minded in its engagements with Nasdaq on our plans to migrate our SCI Systems, up to and including our markets, into a cloud environment. To be clear, such informal discussions and non-objections are preferable to a formal "no" or "not yet," but given the painstaking multi-year planning process and significant investments involved in cloud migration, at least having a clear

---

27 See Division of Trading and Markets, "Responses to Frequently Asked Questions Concerning Regulation SCI," at Question 2.03, last updated August 21, 2019, at https://www.sec.gov/divisions/marketreg/regulation-sci-faq.shtml .

28 See, e.g., FFIEC Information Technology Examination Handbook: Outsourcing Technology Services; at Statement on Outsourced Cloud Computing (July 10, 2012), at https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

29 See FFIEC Statement on Outsourced Cloud Computing (July 10, 2012), at http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf; European Securities and Markets Authority, Guidelines on Outsourcing to Cloud Service Providers, October 5, 2021, at https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf ; UK Financial Conduct Authority, FG 16/5 – Guidance for Firms Outsourcing to the 'Cloud' and Other Third-Party IT Services (July 2016), at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf; Monetary Authority of Singapore, Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption, June 1, 2021, at https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Cloud-Advisory.pdf.

path to "yes" would allow us to proceed with less uncertainty and unease that our decisions and approaches will be upended unexpectedly or second-guessed after the fact.

While we welcome the guidance that the Proposal contains, we question why the Commission chooses to articulate it as dicta within the context of a larger rulemaking, where its regulatory status is unclear. Nasdaq believes that such guidance is more appropriate for publication in a standalone document that itself is made subject to notice and comment that might better serve to refine and strengthen it.

We are also concerned that the Commission's cloud guidance is not as specific and clear as it could or should be. It does too little to specify what the Commission actually wants and expects of SCI Entities in this context and in too many cases, it simply recommends that we consider for ourselves how to address key issues. Below are some examples:

- What does the SEC expect when it says that "SCI entities may want to consider any lock-in effects that utilizing CSP-specific tools might have"? [30] What does the SEC interpret "lock-in" to mean? Does the SEC have in mind any particular steps that SCI Entities should or must take to mitigate this risk?
- What does the SEC have in mind when it states: "it may be useful for SCI entities to consider the relative benefits and costs of potential alternatives that could reduce dependence on any single CSP"? [31] Is the SEC suggesting that SCI Entities must or should pursue multi-cloud strategies?
- The SEC states as follows: "In cases where the use of CSPs is being considered for both primary and backup systems, an SCI entity, taking into account the nature of its systems, may want to consider whether it is appropriate to utilize different CSPs, for such systems, as well as whether an 'on-premises' backup may be appropriate." [32] We know from public filings that in the case of the Options Clearing Corporation, it agreed to maintain such a tertiary on-premises back-up capability in connection with moving its systems into the public cloud, but is the SEC suggesting that such a step would be required of all SCI Entities? And if so, why, if the design of CSPS provide for automatic failovers to geographically diverse regions similar to the geographically-diverse back-up facilities that SCI Entities maintain today?
- What does the SEC mean when it states: "In performing this risk-based assessment, SCI entities would be required to consider third-party provider concentration, which would help ensure that they properly account and prepare contingencies or alternatives for an overreliance on a given third-party provider by the SCI entity or by its industry"? [33] What does the SEC define as "concentration risk"? How much of the industry must be in the cloud or use a

30 Reg. SCI Proposal, supra, at 23178.

31 Id.

32 Id.

33 Id. at 23180.

particular CSP for this risk to emerge? And by what means does it expect or suggest that we address this risk?

- What does the SEC mean when it states as follows: "BC/DR plans generally should not only take into account and address temporary losses of functionality, support, or service – such as a momentary outage that causes a feed to be interrupted or extended cybersecurity event on the third-party provider – but also consider more extended outage scenarios, including if the third-party provider goes into bankruptcy or dissolves, or if it breaches its contract and decides to suddenly, unilaterally, and/or permanently cease to provide the SCI entity's critical SCI systems with functionality, support, or service"? [34] What length of time does the SEC consider to be an extended outage scenario? A month? A year? Something else? And once again, what features does the SEC suggest or require that BC/DR plans must have to address this risk? Must an SRO have a back-up arrangement with another CSP, or maintain a capability to quickly transition back to an on-premises deployment?

These issues are thorny and we appreciate the fact that the SEC does not seek to impose a singular, one-size-fits-all approach to dealing with them, especially where multiple reasonable approaches are possible. Nevertheless, we think that the SEC's guidance should do more to explain the nature of its concerns and provide examples of what it would consider to be acceptable means of addressing those concerns.

Lastly, Nasdaq would like to comment on proposed amendments to Reg. SCI's definition of an "SCI Event." Given the serious nature of cyber-threats, Nasdaq appreciates the Commission's desire to better understand the threat environment, including by having access to more and more timely information about such threats, even where the threats do not materialize into actual or successful attacks that breach or disrupt SCI Systems or cause harm.

Nevertheless, Nasdaq is concerned that the scope of the expanded definitions is too broad and that it would result in Nasdaq having to provide to the Commission an excessive volume of information, the vast majority of which will neither be particularly relevant to our SCI Systems nor actionable to the SEC, even if relevant.

Especially where SCI Entities like Nasdaq utilize large service providers, such as CSPs which have thousands of customers spanning the spectrum of industries and which operate in data centers all over the country and the world, the universe of potential threats is large, varied, and persistent. At any given time, CSPs face and defend against a multitude of threats and attempted breaches and service degradations, most of which are either generalized or directed against targets other than SCI Entities or our SCI Systems. In short, most of the information that we might be required to report under the Reg. SCI Proposal would be irrelevant.

Disclosure of all of these threats on a real-time or near-real-time basis to the SEC would be overwhelming for the SEC and we fear that it would create a misleading sense of the true dangers facing SCI Entities at any given point in time. Although some of these threats are indeed sophisticated and serious, the fact that very few of them succeed or even come close to

---

[34] Id.

affecting customers like Nasdaq should be telling about the reasonableness and effectiveness of the precautions taken.

Real-time disclosure of threat information may be dangerous to the efforts of an SCI Entity, a CSP, or the law enforcement and intelligence agencies with which they coordinate, to prevent or defend against an attack. SCI Entities, CSPs, and government agencies often take time to quietly monitor and analyze threats after detecting them to understand who may be behind them, their objectives, and how to counter or defend against them. The mere revelation that the threat or attack has been detected – particularly before it has determined how to fix for an underlying vulnerability that a threat actor seeks to exploit – may compromise such work and make the threats or attacks more likely to succeed or to spread to others with similar vulnerabilities.

Moreover, existing SCI Event reporting procedures and processes are not designed to handle the real-time processing of large volumes of SCI Events. For SCI Entities like Nasdaq, each assessment of whether an incident constitutes an SCI Event is a time- and resource-intensive effort, as is drafting and filing initial and follow-up notifications to the Commission, and undertaking remediation and a root cause analyses. Although onerous, the current system is manageable because the existing definition of an SCI Event is calibrated carefully to filter out incidents of less immediate concern – that is, either such incidents do not constitute SCI Events at all or they are *de minimis* SCI Events that have lighter reporting and resolution requirements. We fear that the proposed amendments to the definition of an SCI Event would tip this carefully calibrated system out-of-balance and overwhelm SCI Entities and their service providers with the need to grapple with a flood of threat information under exceedingly tight and unforgiving deadlines.

This burden might be warranted if it was clear that the SEC had a productive use for the additional information it seeks. However, it is not apparent what the SEC could or would do with much of this information, other than simply to accumulate it.

With that said, we agree that the SEC should be apprised of significant threats or attempted breaches of SCI Systems, but we believe that the notification obligation should arise once an SCI Entity has reason to conclude that a significant threat or attempt is likely to impact an SCI System specifically and is, in fact, likely to become an SCI Event – notwithstanding any prior or ongoing attempts at prevention or defense. Moreover, SCI Entities should have the ability to delay notification to the extent that and for so long as doing so is reasonably necessary to mitigate ongoing security risks to the SCI System, the SCI Entity, market participants, investors, or the public, or to the extent that federal law enforcement or intelligence agencies instruct it to do so.

The SEC should continue to classify systems intrusions that are unsuccessful or that cause no harm, as *de minimis* events that are to be reported on a quarterly basis, rather than on an immediate basis.

III. New Rule 10 Proposal

Nasdaq wishes to comment specifically on the requirement to disclose publicly summary descriptions of cybersecurity risks and the significant cybersecurity incidents experienced during

the current or previous calendar year on Part II of proposed Form SCIR.[35] The New Rule 10 Proposal states that cybersecurity risk can be addressed through policies and procedures that are reasonably designed to manage the risk. Also, the New Rule 10 Proposal notes that a second means to address cybersecurity risk to the U.S. securities markets is through the Commission gathering and sharing information about significant cybersecurity incidents.[36]

Nasdaq believes that the harm that could result in publicly disclosing the internal weaknesses of a covered entity[37] outweighs the benefit of the Commission's goal of providing customers, counterparties, members, registrants, or users information to better assess the effectiveness of covered entities' cybersecurity preparations. In fact, requiring covered entities to publicly disclose their cybersecurity risks, in a convenient format and location, supplies bad actors with specific intelligence concerning a covered entity's infrastructure that may result in additional harm to that covered entity. Covered entities design policies and procedures to manage their risk. These policies and procedures are not publicly disclosed because of the potential for information leakage. A covered entities' ability to design resilient and effective cybersecurity programs to combat anticipated risks necessarily requires those programs to remain confidential. Disclosing cybersecurity risks necessitates some disclosure of the covered entity's cybersecurity program, policies, procedures and infrastructure. Nasdaq believes disclosing cybersecurity risks to the Commission should be sufficient. In lieu of requiring covered entities to publicly disclose cybersecurity risks, the Commission could publicly disclose cybersecurity risks experienced by covered entities in an aggregated and anonymized format so as not to reveal sensitive information.

IV. Reg S-P Proposal

Nasdaq appreciates the Commission's efforts through its proposed amendments to Reg S-P to update requirements regarding responses to security incidents impacting personal data. For many entities covered by this regulation, we understand that the updated requirements would bring the Commission's requirement into closer alignment with Interagency Guidelines Establishing Standards for Safeguarding Customer Information adopted by federal banking regulators, to align requirements for companies with various entities covered by Commission and banking requirements.

While we appreciate the importance of notifying individuals promptly about incidents impacting their personal data, the "law enforcement" exception to the notification requirement in the Proposal is too narrowly drawn and does not align with similar exceptions in other breach notification regulations. Notifiable incidents affecting personal data can include a wide variety

---

35 See sections II.B.3. and II.B.4.of the New Rule 10 Proposal.

36 See New Rule 10 Proposal at 20280.

37 New Proposed Rule 10 defines a "covered entity" as certain broker-dealers, the Municipal Securities Rulemaking Board, all clearing agencies, national securities associations, national securities exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and transfer agents.

of events ranging from inadvertent mistakes to criminal acts by insiders to ransomware for profit to nation state attacks. In cooperating with law enforcement at the state, federal or global level, an entity may receive a request to refrain from disclosure to individuals to address important law enforcement or national security objectives. An entity responding to an incident should not be placed in a situation where it faces competing requirements from a regulator and law enforcement seeking to apprehend criminal actors or protect vital national interests.

We respectfully request that the exception to reporting be expanded to include documented requests from a competent law enforcement agency for the duration requested by such agency. To the extent that the Commission has concerns about such a request regarding a particular incident, those concerns should be mediated directly between the Commission and the law enforcement agency via intergovernmental mechanisms.

Additionally, we request that the implementation timeline associated with the updated regulation be extended to 24 months following finalization. This implementation timeframe is particularly important in light of the requirements that the Proposals impose on covered entities contracting with service providers. In addition to this Proposal, there are numerous other pending or contemplated regulatory changes related to cybersecurity and resiliency that will likely impact service providers to regulated financial service industry over the near-future. To address such requirements, service providers may need to update their business processes and will be receiving requests from their customer base to update contractual documents. Any implementation timeline should account for level of effort associated with such changes.

* * *

Nasdaq appreciates the opportunity to respond to the Commission's Proposals and applauds the Commission's actions to enhance cybersecurity obligations. While Nasdaq supports the Commission's efforts, it requests the Commission consider a harmonized approach to cybersecurity regulation in finalizing the Proposals.

Thank you for your consideration of our comments. Please feel free to contact me with any questions.

Sincerely yours,

Jeffrey S. Davis