NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.
750 First Street, NE, Suite 990
Washington, DC 20002
202-737-0900
www.nasaa.org

May 22, 2023

**Submitted by SEC Webform (https://www.sec.gov/cgi-bin/ruling-comments)**

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

**RE: File Nos. S7-05-23, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information; S7-06-23, 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; and S7-04-22, Reopening of Comment Period for "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies"**

Dear Ms. Countryman:

On behalf of the North American Securities Administrators Association ("NASAA"),[1] I am writing in response to the following three cybersecurity proposals (collectively, the "Proposals") from the U.S. Securities and Exchange Commission ("SEC" or "Commission"): Release No. 34-97141, *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information* (hereinafter, "Reg. S-P Proposal"); Release No. 34-97142, *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* (hereinafter, "BD Cybersecurity Risk Proposal"); and Release No. 33-11167, *Reopening of Comment Period for "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies,"* reopening comments on prior Release No. IA-5956, *Cybersecurity Risk Management for*

[1] Organized in 1919, NASAA is the oldest international organization devoted to investor protection. NASAA's membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico, the U.S. Virgin Islands and Guam. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

*Investment Advisers, Registered Investment Companies, and Business Development Companies* (Feb. 9, 2022) (hereinafter, "IA Cybersecurity Risk Proposal").[2] With respect to the IA Cybersecurity Risk Proposal, this comment letter supplements a previous comment letter NASAA submitted regarding this proposal on April 11, 2022.[3]

As will be discussed below, NASAA broadly supports the Proposals, but we recommend several revisions prior to adoption. Our most significant recommended revision is for the SEC to develop a single industry-wide disclosure form (*e.g.*, a reformulated and universal version of Form SCIR contained in the BD Cybersecurity Risk Proposal) that could be used by all registrants subject to the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal. Furthermore, this new form should be filed through the Central Registration Depository ("CRD") system and the Investment Adviser Registration Depository ("IARD") system to the maximum extent practicable, with filings on the SEC's Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") system limited to those few SEC registrants that do not otherwise use either CRD or IARD. We recognize that reframing the proposed disclosure structures for the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal could take some time for the SEC to develop and implement. However, we believe the benefits of following this path, which would be akin to the path the SEC previously tread in developing a filing mechanism for Form CRS, would be worth any potential implementation delay.

## I. Introduction

The Reg. S-P Proposal represents a significant update to Regulation S-P, first adopted by the Commission in 2000. The Reg. S-P Proposal would, among other things, strengthen the SEC's regulatory standards in the safeguards rule, Rule 248.30(a), by requiring broker-dealers, investment advisers and certain other registrants (so-called, "covered institutions") to have written policies and procedures reasonably designed to detect, respond to, and recover from any

---

[2] The Proposals are available at https://www.sec.gov/rules/proposed/2023/34-97141.pdf (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information); https://www.sec.gov/rules/proposed/2023/34-97142.pdf (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); https://www.sec.gov/rules/proposed/2023/33-11167.pdf (Reopening of Comment Period for "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies"); and https://www.sec.gov/rules/proposed/2022/33-11028.pdf (Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies). NASAA is consolidating its comments on these Proposals into this single comment letter because of the interconnectedness of the issues raised across all the Proposals.

[3] *See* Letter from NASAA President Melanie Senter Lubin, Re: File No. S7-04-22, Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies (Apr. 11, 2022), https://www.sec.gov/comments/s7-04-22/s70422-20123450-279695.pdf.

unauthorized access or use of their customers' information.[4] Covered institutions would also face a new obligation to notify customers whose information may have been accessed or used improperly, with this new duty standing alongside any other notice requirements that exist under state or federal law.[5] Furthermore, these new policies and procedures would have to contemplate how to safeguard customer information held by a covered institution's outsourced service providers.[6]

The BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal would require covered broker-dealers, investment advisers and other registrants to implement similar internal policies and procedures reasonably designed to address cybersecurity risks facing the registrant. The required procedures would include periodic cybersecurity risk assessments, information system controls, oversight of service providers, and measures to detect, mitigate and remediate cybersecurity threats and cybersecurity incidents.[7] Registrants would be required to provide information about significant cybersecurity incidents confidentially to the SEC and, for some registrants, disclose general information about such incidents publicly. A new SEC form, Form SCIR (Parts I and II), would become an important part of this new cybersecurity reporting and disclosure structure for broker-dealers and other market entities,[8] while investment advisers would use new Form ADV-C.[9] New defined terms and regulatory standards would guide how registrants must devise and implement their new cybersecurity risk management policies and procedures. We begin our comments with recommendations regarding these Proposals. Part II discusses our recommended revisions to the Reg. S-P Proposal. Part III discusses our consolidated recommendations regarding the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal.

## II. Comments on Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information

### *A. Response to Questions 28, 29 and 50: The Customer Cybersecurity Notice Obligation Should Apply Whenever There Has Been an "Actual or Reasonably Possible" Loss or Misuse of Sensitive Customer Information Unless a Covered Institution Concludes it is Not*

---

4 *See* Reg. S-P Proposal 19-20.

5 *See id.* at 15, 5-6.

6 *See id.* at 34-35.

7 *See* BD Cybersecurity Risk Proposal at 51-53; IA Cybersecurity Risk Proposal at 25-30.

8 *See* BD Cybersecurity Risk Proposal at 53.

9 *See* IA Cybersecurity Risk Proposal at 41.

***"Reasonably Likely" that any Customer will be Substantially Harmed or Inconvenienced.***[10]

NASAA recommends the notice obligation in the Reg. S-P Proposal be revised slightly. As proposed, a "covered institution" would be required to notify customers of a cybersecurity incident if it is "reasonably likely" that sensitive customer information held by the covered institution or one of its service providers was accessed or used without authorization and the covered institution cannot conclude that it is "reasonably likely" no customer will face substantial harm or inconvenience as a result. Covered institutions thus would need to make two 'reasonable likelihood' determinations: (i) whether it is reasonably likely sensitive customer information was accessed or used without authorization, and (ii) whether it is reasonably likely that substantial harm or inconvenience to customers could result. NASAA recommends the SEC change the regulatory standard for the first of these two determinations from "reasonably likely" to "reasonably possible."

NASAA believes the lower "reasonably possible" standard should apply to a covered institution's assessment of whether sensitive customer information has been accessed or used without authorization. This lower threshold would make clear that a covered institution has a duty to notify customers in circumstances where the institution knows it has been hacked but the scope of the hack is indeterminate. Under the Reg. S-P Proposal as drafted, a covered institution in such circumstances could reasonably conclude it had no notice obligation because it simply lacked sufficient information to find a "reasonable likelihood" that any customer information was accessed or used without authorization. The higher threshold currently contained in the SEC's proposed standard, coupled with the natural tendency of any business to want to avoid making disclosures that could incur liability or lose customers, leaves open the potential that customers will not be notified of some information security compromises that could threaten their investments. A "reasonably possible" standard is more appropriate to govern this underlying customer notice obligation.

Although we recommend the standard for the initial notice obligation be reduced to "reasonably possible," the SEC should retain the "reasonably likely" standard for the second question, namely whether an unauthorized access or use of information could result in substantial harm or inconvenience to any customer. It is appropriate for this second determination, which

---

[10] *See* Reg. S-P Proposal at 45, Question 28 (*"The proposed standard requires providing notice to affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. . . . Should the trigger for notification be . . . 'reasonably possible' . . .?"*); *id.*, Question 29 ("*A covered institution can rebut the presumption of notification if it determines . . . sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. . . . Should the standard be 'not reasonably possible'?"*); *id.* at 57, Question 50 (*"To the extent covered institutions are not able to determine which individuals are affected with certainty, should the rule require notice only to those individuals whose sensitive customer information was 'reasonably likely' to have been accessed or used without authorization? . . ."*).

amounts to an exception to the underlying notice obligation, to have a higher legal threshold. Our recommended revision is thus intended to yield the following basic governing rule for the new customer notice obligation in the Reg. S-P Proposal: Covered institutions must give notice to any customer whose sensitive customer information actually or reasonably possibly was accessed or used without authorization unless the covered institution concludes it is not reasonably likely that substantial harm or inconvenience to the customer will result. This seems to us to be the correct standard. What is more, this approach would align Regulation S-P more closely to the existing "reasonably possible" notice standards set by federal banking regulators for their registered entities.[11] These are subtle differences from the current text of the Reg. S-P Proposal, and so we have prepared edits to proposed Rule 248.30 in the attached endnote to accomplish this intent.[i]

### *B. Response to Questions 43, 44, 46 and 47: The Definition of "Substantial Harm or Inconvenience" in Rule 248.30 Should Encompass Any Personal Injury or Financial Loss or Any Nontrivial Expenditure of Effort or Loss of Time.*[12]

The phrase "substantial harm or inconvenience" is a key definitional component of the Reg. S-P Proposal. If a cybersecurity incident does not pose "substantial harm or inconvenience" to a customer, no notice is required. Congress used this phrase in Section 501 of the Gramm-Leach-Bliley Act ("GLBA") but did not define it, and this phrase has not been defined by any of the other federal regulators responsible for implementing the GLBA in their own regulatory spheres.[13] Notwithstanding this, the SEC should not shy away from adopting its own definition of this term for the securities industry. Furthermore, we broadly agree with the SEC's proposed definition, albeit with the following recommended revisions.

---

[11] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15752 (Mar. 29, 2005) (hereinafter, "Banking Guidance") (stating notice should be given if "the institution determines that misuse of its information about a customer has occurred or is reasonably possible").

[12] *See id.* at 54, Question 43 (*"Should we expand the proposed definition of 'substantial harm or inconvenience'? Alternatively, should we exclude some harms covered under the proposed definition? . . ."*); *id.* Question 44 (*"Do commenters believe that the proposed rule should reference a term or terms other than 'substantial' and 'more than trivial' in describing the types of harms that meet our definition? . . ."*); *id.* at 55, Question 46 (*"Should a harm that is a 'personal injury,' such as physical, emotional, or reputational harm, only be included in the proposed definition if it is more than 'trivial,' similar to our proposed treatment of financial loss, expenditure of effort or loss of time? . . ."*); *id.* Question 47 (*"What kinds of financial loss, expenditure of effort or loss of time would individuals likely be unconcerned with and/or likely not to try to mitigate? . . ."*).

[13] *See* Section 501, Pub. Law. 106-102, 113 Stat. 1338 (Nov. 12, 1999). *See also* Reg. S-P Proposal at 53; Banking Guidance, *supra* note 11 (discussing but not defining "substantial harm or inconvenience"); National Credit Union Administration, Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, 70 Fed. Reg. 22764 (May 2, 2005) (same); Federal Trade Commission, Standards for Safeguarding Customer Information, 67 Fed. Reg. 36484 (May 23, 2002) (same); Commodity Futures Trading Commission, Privacy of Consumer Financial Information, 66 Fed. Reg. 21236 (Apr. 27, 2001) (same).

First, the SEC should revise its proposed definition of "substantial harm or inconvenience" to remove the requirement that personal or financial harms must be nontrivial. The SEC's proposed definition begins, "*Substantial harm or inconvenience* means personal injury, or financial loss, expenditure of effort or loss of time that is more than trivial . . . ." The concept of nontriviality is thus a limiting factor in all three types of enumerated customer harms: personal injuries, financial losses, and expenditures of effort / losses of time. Nontriviality should only apply to the third of these potential harms, though.

The concept of nontriviality should not limit the scope of potential personal or financial harms because there might always be some set of individuals to whom a particular personal or financial harm is material. Securities firms should not be put into the untenable position of attempting to determine what potential personal or financial harms to their customers are significant enough to require customer notice. Instead, potential personal or financial harms should always be notice-worthy. In contrast, it is reasonable to apply the concept of nontriviality to cabin the scope of potential harms or inconveniences that would infringe upon a customer's time and personal labors. Customers would consider risks to their person and their pocketbook to be materially distinct from risks to their time and energies.

Second, the definition of substantial harm or inconvenience should include the term "cyberattack" as one of the enumerated events that could give rise to the customer notice obligation. The SEC's current definition includes "theft" and "fraud" as events that could trigger customer notice, but these general terms do not capture the same potential scope of conduct as the word "cyberattack." For example, the Computer Security Resource Center of the National Institute of Standards and Technology defines a cyberattack as any "malicious activity that attempts to collect, disrupt, deny, degrade or destroy" information or data.[14] We have reflected all our recommended revisions to the definition of "substantial harm or inconvenience" in the attached endnote.[ii]

### *C. Response to Questions 34, 35, 66 and 67: The Form of Customer Notices Should Not be Prescribed, and the SEC Should Remind Registrants About the Existing Intersections Between Regulation S-P and State Data Breach Notification Laws.*[15]

---

[14] *See* https://csrc.nist.gov/glossary/term/Cyber_Attack.

[15] *See* Reg. S-P Proposal at 46, Question 34 (*"Under what scenarios would a covered institution be unable to comply with both the proposed rules and applicable state laws? Please explain."*); *id.*, Question 35 (*"Should the proposed rules be modified in order to help ensure covered institutions would not need to provide multiple notices in order to satisfy obligations under the proposed rules and similar state laws?"*); *id.* at 69, Question 66 (*"Should we incorporate other prescriptive formatting requirements (e.g., length of notice, size of font, etc.) for the notice requirement under the proposed rules?"*); *id.*, Question 67 (*"Should we require covered institutions to follow plain English or plain writing principles?"*).

The Reg. S-P Proposal also seeks comment on the proposed format of customer notices and the implications of this requirement on state data breach notification laws. NASAA broadly agrees with the Reg. S-P Proposal as drafted on these issues.

With respect to the form of customer notices, we agree with the Reg. S-P Proposal that the SEC should not be prescriptive. This is not an issue for which the SEC should prescribe specific standards. Rather, it is entirely appropriate for securities firms to prepare their own notices in whatever format reasonably fulfills their legal obligations and extends their desired courtesies to customers. In addition, not prescribing a format for customer notices will make it easier for covered institutions to fulfill all their notice obligations under federal and state laws with as few notice documents as possible (ideally through a single notice to all affected customers nationwide). Being prescriptive here could potentially create inconsistencies with current or future state notice laws, which in turn could cause covered institutions to feel compelled to deliver entirely duplicative notices to customers simply for reasons of form. Customers should not be burdened in this way, and the Reg. S-P Proposal rightly takes this into account.[16]

In addition, with respect to the intersections between the proposed notice requirements in SEC Rule 248.30 and state data breach notification laws, we encourage the SEC to remind registrants about existing SEC Rule 248.17. Rule 248.17, adopted by the Commission in 2000, restates Section 507 of the GLBA to make clear that Regulation S-P does not preempt state law (except to the extent of any inconsistencies between the two).[17] The new customer notice obligation in Rule 248.30 will also be governed by this principle. However, the Reg. S-P Proposal does not mention this SEC rule. We encourage the SEC to remind registrants about Rule 248.17 to avoid potential confusion regarding the impact of new Rule 248.30 on existing state notice laws; it would be unfortunate if an SEC registrant mistakenly thought Rule 248.30 set forth its only customer notice obligations.[18] Relatedly, we see no reason covered institutions would be unable to comply with Rule 248.30 and state notice laws, particularly if the SEC does not mandate the form of disclosures under Rule 248.30.

---

16 *See id.* at 44.

17 *See* Privacy of Consumer Financial Information (Regulation S–P), SEC Rel. No. 34-42974 (Jun. 22, 2000), 65 Fed. Reg. 40334, 40356 (Jun. 29, 2000).

18 Some state notice laws include the potential for private rights of action, which registrants also should be mindful of.

## III. Comments on the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal

This portion of our comment letter contains NASAA's consolidated responses to the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal (and supplements our April 11, 2022, comment letter on the IA Cybersecurity Risk Proposal).[19]

### *A. Cybersecurity Disclosures for Regulated Entities Should be Made on a Universal Filing Form (Such as Form SCIR) Submitted Principally via the CRD and IARD Systems and via EDGAR Only for Market Entities Not Otherwise Required to Use CRD or IARD.*

NASAA supports the requirements in the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal for regulated entities to implement cybersecurity risk management procedures and report on significant cybersecurity incidents to the SEC and to the marketplace at large. NASAA recommends a change in how the Commission proposes to implement these new disclosure requirements.

As currently drafted, the BD Cybersecurity Risk Proposal would require broker-dealers and other market entities to give immediate notice of significant cybersecurity events to the SEC, followed promptly thereafter by more fulsome confidential disclosures on Form SCIR Part I. These reports would be filed on EDGAR.[20] Many broker-dealers also would be required to make periodic public disclosures of their cybersecurity risk management policies and significant cybersecurity incidents they have faced through Form SCIR Part II.[21] The IA Cybersecurity Risk Proposal would separately require investment advisory firms to report publicly on their cybersecurity risk management policies and significant cybersecurity incidents via Form ADV-C filed on the IARD system.[22]

Rather than having two separate forms on separate filing platforms, the SEC should instead follow the path it undertook when developing Form CRS and create a single industry-wide cybersecurity reporting form filed principally (if not universally) on the interrelated CRD and IARD systems. We believe it would be preferable for all registrants subject to the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal to file their required confidential and public cybersecurity disclosures on a shared form (such as a revised version of Form SCIR). Furthermore, the CRD system and the IARD system should be the platform for

---

19 *See supra* note 3.

20 *See* BD Cybersecurity Risk Proposal at 134.

21 *See* BD Cybersecurity Risk Proposal at 56.

22 *See* IA Cybersecurity Risk Proposal at 50.

these filings, with filings on EDGAR limited to those market entities that do not (or cannot) otherwise use CRD or IARD.[23]

A single industry-wide form filed on CRD and IARD would simplify the overall filing process, particularly for dually-registered broker-dealers and investment advisers. It would also be easier for regulators and the public at large to review these disclosures and compare disclosures across multiple registrants if they were consolidated onto the interrelated CRD and IARD platforms. We recognize that implementing this change could necessitate a delay in the new cybersecurity reporting regime, potentially requiring the Commission to undertake an entirely new round of public notice and comment. But we believe the benefits of doing this would outweigh the downsides, making this a change well worth waiting for.[24]

A universal cybersecurity disclosure form filed through CRD and IARD would have other benefits beyond streamlining the basic filing process. First, this would simplify the delivery of required cybersecurity disclosures to regulatory agencies. The Commission proposes in the BD Cybersecurity Risk Proposal that market entities deliver their Form SCIRs to the SEC and to their primary examining authorities (if they have one).[25] Putting these disclosures onto CRD would simplify this process, as both the SEC and a registrant's examining authority would have immediate access to the disclosures on CRD.[26] Second, filing these disclosures on CRD and IARD would make the nonpublic disclosures (*e.g.*, Part I of Form SCIR) available for review

---

[23] For example, some transfer agents, including those registered as national banks, may not currently be required to use CRD for any reason. These entities should be able to continue using EDGAR as their sole platform for regulatory filings to the SEC. *See* Transfer Agents, SEC (last modified Apr. 28, 2016), https://www.sec.gov/divisions/marketreg/mrtransfer; Electronic Filing of Transfer Agent Forms, SEC Rel. No. 34-54864 (Dec. 4, 2006), *available at* https://www.sec.gov/rules/final/2006/34-54864.pdf.

[24] As an aside, it is worth noting that when the SEC first proposed Form CRS, it planned for broker-dealers to file Form CRS on EDGAR and for investment advisers to file Form CRS on IARD. *See* Form CRS Relationship Summary; Amendments to Form ADV; Required Disclosures in Retail Communications and Restrictions on the use of Certain Names or Titles, SEC Rel. No. 34-83063, at 16 (Apr. 18, 2018), *available at* https://www.sec.gov/rules/proposed/2018/34-83063.pdf. NASAA and other commenters responded that CRD would be a better platform for broker-dealers to use, given that CRD has traditionally been the platform for broker-dealer regulatory disclosures (including confidential disclosures). *See* Letter from NASAA President Joseph P. Borg, Re: Consolidated Comments in Response to SEC Proposed Rulemakings, at 16 (Aug. 23, 2018), *available at* https://www.sec.gov/comments/s7-07-18/s70718-4259557-173080.pdf. The SEC ultimately agreed, writing in its Form CRS adopting release that CRD and IARD are "currently used by and familiar to broker-dealers and investment advisers" and that filing on CRD and IARD should "minimize the [internal] system changes firms would need to make" to comply with this new filing requirement. *See* Form CRS Relationship Summary; Amendments to Form ADV, SEC Rel. No. 34-86032, at 203-04 (Jun. 5, 2019), *available at* https://www.sec.gov/rules/final/2019/34-86032.pdf. We believe the same logic and the same basic result should apply here. The ability to file the disclosures on EDGAR should be limited to those market entities that do not have to use CRD or IARD for any other reason.

[25] *See* BD Cybersecurity Risk Proposal at 134.

[26] *See id.* at 137 (stating a registrant would be required to "transmit a copy" of any Form SCIR it files with the SEC to its examining authority but not specifying how such communications would be made).

by other regulators, including NASAA's member state securities regulators.[27] It would be appropriate for state securities regulators to have access to these confidential cybersecurity disclosures alongside the SEC so that state regulators could conduct their own reviews and analyses of this information, monitoring for cybersecurity risks affecting their particular jurisdictions or state registrants, and responding to inquiries from affected persons within their jurisdiction. Expanding regulatory access to these new cybersecurity disclosures would be profoundly beneficial for the safety of the securities markets, registrants, and the investing public.

### *B. Response to BD Cybersecurity Risk Proposal Question 75: Non-Covered Broker-Dealers Should be Required to File Form SCIR Parts I and II (Like All Other Market Entities).*[28]

The BD Cybersecurity Risk Proposal would create two categories of broker-dealers, termed covered broker-dealers and non-covered broker-dealers. Covered broker-dealers would broadly include larger brokerage firms and broker-dealers that maintain custody of customer securities, while non-covered broker-dealers would generally consist of smaller firms and firms that limit their activities to niches such as facilitating private placements or selling mutual funds and variable annuities.[29] Both types of brokers-dealers would be required to implement cybersecurity risk management procedures, conduct annual internal cybersecurity reviews, and provide prompt notice to the SEC of any significant cybersecurity incidents they face,[30] though non-covered broker-dealers would enjoy relaxed cybersecurity risk management standards and would be excused from the requirement to file new Form SCIR (both the confidential Part I and the public Part II).[31] The SEC's rationale for distinguishing non-covered broker-dealers on these issues is that non-covered broker-dealers will be less likely than covered broker-dealers to maintain confidential customer information and non-covered firms generally will be smaller and have less complex information technology systems.[32]

---

[27] Based on our familiarity with the CRD and IARD platforms, we believe it would be possible to code the system such that the cybersecurity disclosures could be made available to regulators as broadly, or as narrowly, as the Commission desired. We favor broad access of these disclosures to federal and state regulators, as we believe all regulators could make good use of this information in furtherance of their respective market oversight and investor protection missions.

[28] *See* BD Cybersecurity Risk Proposal at 190, Question 75 (*"Should paragraph (e)(1) of proposed Rule 10 be modified to specify certain minimum elements that would need to be included in the policies and procedures of Non-Covered Broker-Dealers? . . ."*).

[29] *See id.* at 63-64.

[30] *See id.* at 51-53.

[31] *See id.* at 184-85. Non-covered broker-dealers would still have to provide "immediate written notice" of cybersecurity incidents confidentially to the SEC, though. *See id.* at 374.

[32] *See id.* at 186.

NASAA has no objection to aligning cybersecurity risk management standards where the risks are lower such as at non-covered broker-dealers. The potential customer harms that could arise from a cybersecurity incident at a non-covered broker-dealer, which by definition cannot have custody of client funds, are lower than those raised by a covered broker-dealer. Furthermore, some non-covered broker-dealers (such as private investment banking firms) may not even have a single individual client among its customer base. Requiring these types of firms to implement the same degree of cybersecurity risk management practices as covered broker-dealers would be an unnecessary burden. Ultimately, the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal make clear that registrants are responsible for devising their own cybersecurity procedures reasonably tailored to meet the needs of their own businesses.[33]

Although we have no objection to setting different regulatory standards for cybersecurity risk management policies at covered versus non-covered broker-dealers, we believe non-covered broker-dealers should not be exempted from the requirement to prepare and file Form SCIR (both Parts I and II). In keeping with our recommendation above that Form SCIR form the basis for a new market-wide cybersecurity disclosure regime, non-covered broker-dealers should also be included especially because many of these firms are likely to have large numbers of retail investors. We see no principled reason to exclude them. The private and public disclosures on Parts I and II of Form SCIR would be equally valuable information to regulators and the public at large for both covered and non-covered firms. If a non-covered broker-dealer has individual customers as clients, it would be subject to the separate cybersecurity notice obligations set forth in the Reg. S-P Proposal.

### *C. Response to BD Cybersecurity Risk Proposal Question 10 and IA Cybersecurity Risk Proposal Definition of "Cybersecurity Incident": Clarify that Authorized Acts Could Cause a Cybersecurity Incident.*[34]

The BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal define a new term, "cybersecurity incident," as a foundation for their new cybersecurity risk management and reporting regimes.[35] Notably, both definitions include the adjective 'unauthorized': "Cybersecurity incident means an *unauthorized* occurrence . . . ."[36] We recommend this definition be revised to clarify that authorized but unintended events could also cause a

---

33 *See* BD Cybersecurity Risk Proposal at 97, 378; IA Cybersecurity Risk Proposal at 10.

34 *See* BD Cybersecurity Risk Proposal at 89, Question 10 (*"Should . . . [we] revise the definition of 'cybersecurity incident'? . . ."*); IA Cybersecurity Risk Proposal at 198 (proposed definition of "cybersecurity incident").

35 *See* BD Cybersecurity Risk Proposal at 479; IA Cybersecurity Risk Proposal at 219.

36 *See supra* note 32.

cybersecurity incident (and thereby potentially result in a disclosable significant cybersecurity incident).

We are confident that the vast majority of cybersecurity incidents will arise from an unauthorized act, such as an external cyberattack or an internal theft of data by a corporate employee. But we do not believe all cybersecurity incidents will necessarily arise this way. Indeed, we can imagine some cybersecurity incidents might arise from completely volitional corporate acts, such as deploying new computer software that inadvertently results in the public disclosure of confidential customer data or such data being available to employees who are otherwise not entitled to access it. Limiting the definition of cybersecurity incidents to only those arising through unauthorized actions could give a registrant cover for not disclosing such a mistake.[37] Furthermore, we believe it is not essential for the definition of "cybersecurity incident" to be limited solely to unauthorized events, given that this word is used elsewhere in the Proposals (including in the definitions of "significant cybersecurity incident" and "cybersecurity threat"). Thus, we would recommend this definition be revised to include unauthorized or *authorized but unintended* acts. The attached endnote contains revisions to Rule 242.10 that would accomplish this intent (and we would recommend conforming revisions to the IA Cybersecurity Risk Proposal).[iii]

### *D. Response to BD Cybersecurity Risk Proposal Question 17 and IA Cybersecurity Risk Proposal Definitions of "Significant Fund Cybersecurity Incident" and "Significant Adviser Cybersecurity Incident": Clarify that Any Customer Notices Made Under Regulation S-P Will Qualify as Significant Cybersecurity Incidents Requiring Notice to Regulators and the Public on Form SCIR.[38]*

The Reg. S-P Proposal would create a new requirement for securities firms to give notice to their customers whenever customer information is accessed or used without authorization and customers could face substantial harm or inconvenience as a result. We believe that any event that causes a firm to give notice to its customers under the Reg. S-P Proposal should also necessarily qualify as a "significant cybersecurity incident" for purposes of the BD

---

[37] It is also noteworthy that the National Institute of Standards and Technology ("NIST") Glossary and the Federal Information Security Modernization Act ("FISMA") do not include the adjective "unauthorized" (or any similar caveat) in their respective definitions of "cybersecurity incident," perhaps for this reason. *See* BD Cybersecurity Risk Proposal at 71, fn. 168.

[38] *See* BD Cybersecurity Risk Proposal at 92, Question 17 (*"Should paragraph (a)(10) of proposed Rule 10 be modified to revise the definition of 'significant cybersecurity incident'? . . ."*); IA Cybersecurity Risk Proposal at 199 (proposed definition of "significant fund cybersecurity incident"); and *id.* at 213 (proposed definition of "significant adviser cybersecurity incident").

Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal.[39] But, as the Proposals are currently drafted, it appears that this is not necessarily so; it appears some disclosable events under the Reg. S-P Proposal could still be non-reportable under the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal.[40] There should be no such gap.

We believe any cybersecurity incident that compels a firm to give notice to its customers should also compel the firm to notify its regulators. This would ensure regulators are not left with less information than a firm's customers and avoid placing a regulator in a position where it cannot answer investor inquiries. What is more, ensuring that no such disclosure gap can exist would obviate the potential for customer confusion between a firm's individual notices to customers and published cybersecurity disclosures. A customer would be understandably confused if they received notice from their brokerage firm that their personal information was accessed or used improperly and yet the brokerage firm reported no significant cybersecurity incidents during that reporting period on its Form SCIR Part II. This potential disclosure gap can be closed by simply incorporating the defined term "substantial harm or inconvenience" from the Reg. S-P Proposal into the definition of "significant cybersecurity incident" in the cybersecurity risk management proposals. We have drafted an edit to Rule 242.10 in the BD Cybersecurity Risk Proposal to accomplish this (and analogous revisions could be made with respect to the IA Cybersecurity Risk Proposal).[iv]

## IV. Conclusion

For the reasons described above, NASAA supports the Proposals and encourages their adoption. We believe the Proposals stand to benefit retail investors and the securities marketplace more generally. However, we recommend that the SEC implement the revisions outlined above before adopting the Proposals. In particular, we recommend the SEC revisit its proposed filing structure for the new cybersecurity risk management disclosures in the BD Cybersecurity Risk Proposal and the IA Cybersecurity Risk Proposal.

---

[39] The IA Cybersecurity Risk Proposal, of course, uses the separate terms "significant *fund* cybersecurity incident" and "significant *adviser* cybersecurity incident." For simplicity, we refer here only to the definition of "significant cybersecurity incident." But if the SEC adopts our recommendation and consolidates the BD Cybersecurity Risk Proposal and IA Cybersecurity Risk Proposal into a single consolidated reporting regime, this revised definition of "significant cybersecurity incident" could be incorporated into both proposals.

[40] This potentiality arises because customer notices under the Reg. S-P Proposal are predicated on the potential that a cybersecurity incident could cause "substantial harm or inconvenience" to one or more customers whereas the definition of "significant cybersecurity event" in the cybersecurity risk management proposals requires "substantial harm." A cybersecurity incident that merely posed a *substantial inconvenience* to customers would not necessarily require regulatory notice under the two cybersecurity risk management proposals. *See* BD Cybersecurity Risk Proposal at 480-81 (definition of "significant cybersecurity incident"); IA Cybersecurity Risk Proposal at 199 (definition of "significant fund cybersecurity incident"); *id.* at 213 (definition of "significant adviser cybersecurity incident").

Should you have any questions about this letter, please contact either the undersigned or NASAA's General Counsel, Vince Martinez, at (202) 737-0900.

Sincerely,

Andrew Hartnett
NASAA President and
Deputy Commissioner,
Iowa Insurance Division

## Endnotes

[i] We recommend the following revisions to the "reasonably likely" determinations set forth in proposed Rule 248.30:

(b)(3)(iii): *Notify each affected individual whose sensitive customer information actually or reasonably possibly was~~, or is reasonably likely to have been,~~ accessed or used without authorization in accordance with paragraph (b)(4) of this section unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.*

(b)(4)(i): *Unless a covered institution has determined, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience, the covered institution must provide a clear and conspicuous notice to each affected individual whose sensitive customer information actually or reasonably possibly was ~~is reasonably likely to have been~~ accessed or used without authorization. The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing.*

(b)(4)(ii): *Affected individuals. If an incident of unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, but the covered institution is unable to identify which specific individuals' sensitive customer information has been accessed or used without authorization, the covered institution must provide notice to all individuals whose sensitive customer information resides in the customer information system that actually or reasonably possibly was~~, or was reasonably likely to have been,~~ accessed or used without authorization.*

(b)(4)(iii): *Timing. A covered institution must provide the notice as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information actually or reasonably possibly has occurred ~~or is reasonably likely to have occurred~~ unless the Attorney General of the United States informs the covered institution, in writing, that the notice [. . .].*

[ii] We recommend the following revisions to the definition of "substantial harm or inconvenience" set forth in proposed Rule 248.30:

(e)(11): *Substantial harm or inconvenience means any personal injury, ~~or~~ financial loss~~,~~ or nontrivial expenditure of effort or loss of time ~~that is more than trivial,~~ to or by an individual arising from any ~~including~~ theft, fraud, cyberattack, harassment, physical harm, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or ~~the~~ other misuse of information identified with ~~an~~ the individual, including any attempt to obtain a financial product or service~~,~~ or to access, log into, effect a transaction in, or otherwise misuse the individual's account.*

[continued]

---

[iii] We recommend the following revisions to the definition of "cybersecurity incident" set forth in proposed Rule 242.10:

(a)(2) *Cybersecurity incident means an unauthorized or authorized but unintended 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.*

[iv] We recommend the following revisions to the definition of "significant cybersecurity incident" set forth in proposed Rule 242.10:

(a)(10) *Significant cybersecurity incident means 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 information or information systems results in or is reasonably likely to result in:*

*(A) Substantial harm to the market entity; or*

*(B) Substantial harm or inconvenience to ~~a~~ any customer~~,~~ or substantial harm to any counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.*