Mark Quinn
DIRECTOR OF REGULATORY AFFAIRS

VIA E-Mail and UPS Overnight

November 26, 2018

Andrea Seidt, Esq.
Investment Adviser Section Chair
Ms. Elizabeth Smith
Investment Adviser Regulatory Policy and Review Project Group Chair
C/O NASAA Legal Department
750 First Street, NE, Suite 1140
Washington, DC 20002

Re: Proposed Investment Adviser Model Rule for Information Security and Privacy Under the Uniform Securities Acts of 1956 and 2002

Dear Commissioner Seidt and Ms. Smith:

Please allow this to serve as comments on behalf of Cetera Financial Group ("Cetera") regarding the proposed Investment Adviser Model Rule for Information Security and Privacy Under the Uniform Securities Acts of 1956 and 2002 (the "Proposed Rule"). Cetera is the corporate parent of a group of six Registered Investment Advisors ("RIAs") with more than 6,000 affiliated representatives. All of our RIA subsidiaries are federally-registered, but we submit these comments as parties that are interested in all state and federal regulations applicable to RIAs and financial advisers in general.

We will offer comments with respect to specific parts of the Proposed Rule below, but in general, we believe that it represents the correct approach to regulation of information security and data privacy. The regime embodied in the Proposed Rule incorporates and builds upon current protocols to which many RIAs are already subject. In addition, it is largely principles-based and allows regulated entities flexibility to adopt policies and procedures that are tailored to the size and complexity of their businesses. We believe that this is critical given the variation in size and available resources of the firms that would be subject to this regulation.

655 W Broadway, 12th Floor
San Diego, CA 92101
mark.quinn@cetera.com

We offer the following comments with respect to specific portions of the Proposed Rule:

1. **Any new regulations relating to data security and privacy should expressly recognize the existing regime of other authorities and promote consistency between the Proposed Rules and those of other agencies**.

   The role of electronic data in all businesses has evolved rapidly over the past 20 years. NASAA is correct in taking this opportunity to set standards for state-registered RIAs. The regime established by the Gramm-Leach-Bliley Act and the SEC in Regulation S-P has been in place for some time and has generally proved to be workable for federally-registered RIAs. The Proposed Rule wisely incorporates and builds upon this framework. Rules applicable to state and federally registered RIAs are not always the same, but in this area, we believe they should be as consistent as possible. We endorse the NASAA approach, especially to the extent that it explicitly recognizes the virtue of consistency among regulatory agencies. We strongly suggest that any future efforts follow that approach.

2. **The principles-based approach embodied in the Proposed Rule is the correct one.**

   At present, there are more than 15,000 state-registered RIAs that would be subject to the Proposed Rule. They range from very small firms with one or two employees that perform limited functions such as financial planning to larger companies that actively manage securities and other assets for substantial numbers of clients. The degree to which they utilize and share data with clients and other entities depends largely upon their size and business model. The Proposed Rule appropriately recognizes the wide universe of entities that will be subject to it and allows flexibility for firms to assess their own needs and capabilities and design processes that are appropriate to their situations. This is especially critical for smaller entities that may have few employees, perform limited functions, or do not share data through electronic means. A "one size fits all" approach could unduly penalize smaller firms and would have undesirable side-effects.

3. **Covered RIAs should be allowed to deliver summaries of privacy policies and periodic updates to clients by electronic means unless the client specifically requests otherwise.**

   Section I (b) of the Proposed Rule establishes a requirement that all covered RIAs deliver a written statement describing the firm's privacy policy to clients upon establishment of their relationship. The summary must be delivered no less frequently than once per year thereafter, and more frequently if the firm makes material changes to its policies. We support the requirement that firms be required to provide written privacy policies to clients, including updates. However, we believe that the Proposed Rule should explicitly

provide that RIAs are permitted to deliver such updates via electronic means such as e-mail, text or instant messaging, and websites. Firms should also be permitted to publish annual or other periodic updates on websites, and such publication should satisfy the annual delivery requirement.

At present, SEC and state rules with respect to electronic delivery of communications to clients vary widely. While most investment advisory accounts that are opened today permit electronic delivery of documents, there are a vast number of "legacy" accounts that were established prior to the time that electronic delivery became a standard. New regulations such as the Proposed Rule would be applicable to all accounts, not just those that are established after it becomes effective.

We believe that the concepts of electronic delivery and "access as delivery" are worthy of a complete re-evaluation by both state securities regulators and the SEC, but we recognize that this may not be the time or forum for such a discussion. We would instead recommend that, with respect to the limited function of providing periodic updates to privacy policies, the Proposed Rule explicitly state that covered RIAs may satisfy their delivery obligations by publication on a firm website to which all customers have access, unless the client specifically requests delivery in hard copy. We would note that Privacy policies generally do not change substantially on an annual basis. Requiring RIAs to deliver hard-copy documents represents a costly and resource-intensive process that does not produce a commensurate benefit for clients. These resources are better devoted to other investor protection-related efforts.

4. **The Proposed Rule should explicitly state that violations do not create private rights of action for customers or other parties in civil litigation.**

As mentioned above, Cetera endorses the principle of establishing standards for data privacy and security. Such standards should be codified in a way that will allow state regulatory authorities to enforce compliance by regulated firms. However, it is an unfortunate reality that breaches of data security happen on a regular basis, to firms large and small. It is also clear that the ability of criminals or others to create "cybermischief" is evolving faster than the ability of anyone to stop them.

The primary purpose of the Proposed Rule should be to encourage and enforce compliance with reasonable standards, with the goal of preventing breaches and avoiding harm to customers or others. Unfortunately, any standard that is codified as part of a state law or regulation will inevitably be cited as evidence of legislative or regulatory intent to confer a private right of action on private parties in the event of a data breach or other similar incident.

If the intent to confer private rights of action is not explicitly addressed in the Proposed Rule, private litigants will almost certainly plead it in claims against

RIAs. This will result in at least two negative consequences: First, to the extent that the Proposed Rule itself does not address the issue of private rights of action, it will be necessary to decide that issue in litigation. Interpreting the intent of any regulation is difficult, and that exercise will result in unnecessary and unproductive litigation if it is not made explicit in the text of the Proposed Rule. More importantly, if a private right of action is created, it will inevitably lead to increased cost for RIAs to manage and resolve claims. Such costs are almost always passed on to clients in some form. It is preferable that this issue be addressed at the outset.

There will be other undesirable effects if the issue of private rights is not addressed in the Proposed Rule. Among other things, RIAs will be more likely to conduct cursory review of their systems, policies and procedures, and to avoid close examination of the causes and effects of breaches for fear of creating a record for claimants to use in litigation. To encourage robust self-examination and reporting, the Proposed Rule should explicitly state that that it is being adopted to enhance regulatory oversight, and that it is not intended to create a private right of action for any claimant.

We do not suggest any other form of limitation on the ability of any claimant to bring legal action. If permissible under other applicable law, claimants should be allowed to pursue any other available theory of recovery.

****

We appreciate the opportunity to comment on this important initiative and look forward to engaging with you on development and implementation of regulations. If we may offer any further information or assistance, please let me know.

Sincerely,

Mark Quinn
Director of Regulatory Affairs
Cetera Financial Group