August 25, 2017

Via e-mail to Andrea.Seidt@com.state.oh.us
Elizabeth.Smith@dfi.wa.gov
nasaacomments@nasaa.org

Re: Response to the NASAA's Request for Public Comment Regarding the Proposed Amendment to the NASAA's Model Rule on Unethical Business Practices of Investment Advisers and Investment Adviser representatives and Federal Covered Advisers

Dear Sir or Madame:

SigFig Wealth Management, LLC ("SigFig" or "we") appreciates the opportunity to respond to the NASAA's Request for Public Comment regarding a proposed model rule amendment to the Unethical Business Practices of Investment Advisers and Investment Adviser Representatives and Federal Covered Advisers NASAA model rule to include investment advisers' accessing client accounts with the client's own unique identifying information (such as username and password) into the list of unethical business practices ("Proposed Rule Amendment" or "Amendment").

SigFig is an investment adviser registered with the U.S. Securities and Exchange Commission ("SEC") and, as such, a fiduciary under the Investment Advisers Act of 1940 ("Advisers Act"). We take our fiduciary duty very seriously and strongly support regulators' initiatives to enforce the fiduciary standard or provide guidance to investment advisers on how to meet their obligations to clients. However, we believe that the Proposed Rule Amendment, if adopted as is, will have significant negative consequences for investors and investment advisers.

Specifically, we think that the Proposed Rule Amendment does not address the fact that there may be different levels of adviser's access to client accounts, some of which would mitigate or not give rise to the concerns as presented by the NASAA in the Request for Public Comment. Further, there are alternative methods that can effectively address the investor protection concerns noted by the NASAA. Finally, the Proposed Rule Amendment does not account for the benefits the practice of accessing client accounts creates for both investors and advisers. We respectively request that the NASAA consider our concerns in these three areas.

I. The Definition of "Access"

SigFig noted that the Proposed Rule Amendment talks about adviser's practice to access client accounts with client's own unique identifying information, such as username and password. However, the Amendment and the Request for Public Comments do not define what constitutes

"access" and do not discuss that there might be different levels of access an adviser can have to client accounts.

In its Request for the Public Comments, the NASAA stated that when an adviser accepts or asks a client for their own usernames and passwords and subsequently accesses client account, the adviser is impersonating the client and has the same access to the account as the client. We disagree with this assertion. For instance, an advisor may utilize a third-party service, which encrypts clients' institutional credentials, while providing read-only account information to the advisor. In this scenario, the adviser has the ability to view the account information (useful in providing quality advice), however, it does not have means to un-encrypt the credentials kept by the third-party provider and access the account on client's behalf, nor perform transactions to "impersonate" the client.

The adviser's access to the client account in a "view-only" format is equivalent to the client providing the adviser with a copy of their account statement and does not raise the same investor protection concerns as the ability to log into the account on the client's behalf using their credentials. Therefore, the Proposed Rule Amendment should provide a definition of "access" or otherwise address the outlined concern.

II. Methods to Address the Investor Protection Concerns

In its Request for Public Comment, the NASAA expressed three main investor protection concerns regarding the advisers' practice of accessing client accounts using client's identifying information, such as usernames and passwords. First, the NASAA indicated that an adviser's access of client accounts using their credentials can give the adviser custody over such client's assets. Second, the Association raised a concern with respect to recordkeeping and, in particular, potential absence of the records to distinguish instances of log-ins by the adviser and the client. Finally, the NASAA stated that such practice could cause clients to violate their user agreements with the entities that provide the login credentials and, consequently, deprive the clients of online account fraud protections.

A. Custody of Clients' Assets

SigFig agrees with the NASAA's determination that the adviser access to clients' accounts will generally rise to the level of having custody if the adviser has authority to obtain possession of (or the ability to appropriate) client funds or securities. The condition of having authority to obtain possession of clients' assets is important. As discussed above, it is unlikely that the adviser's "read-only" access to the account information obtained using encrypted client's credentials would give it the ability to obtain possession of the account funds or securities and, thus, raise custody concerns.

SigFig believes that advisers engaging in practice of accessing client accounts using their credentials already have an obligation to assess the level of such assess and authority it gives with respect to the account funds. This obligation derives from the overall fiduciary responsibility as well as Rule 206(4)-2 of the Adviser Act ("Custody Rule") supplemented by the SEC's guidance, no action letters and FAQs clarifying the Custody Rule. In the event, if an

adviser's access level gives the adviser an ability to obtain possession of clients' assets, it would be subject to Rule 206(4)-2, including the requirement to undergo an annual surprise audit. In our view, compliance with Rule 206(4)-2 addresses a concern that by having access to client accounts the adviser could engage in fraudulent or deceitful conduct, including misappropriation of client's funds or securities.

B. Recordkeeping

Similar to the custody issue, concerns around recordkeeping arise in cases where the adviser has the ability to log into the client accounts on their behalf. SigFig supports the importance of having an audit trail to distinguish between adviser's and client's log-ins. We believe that this issue can be addressed through internal security controls, including the encryption of the provided user credentials, role-based access restrictions, and pre-approval of instances where the adviser needs to access the account on the client's behalf.

C. Violation of Clients' User Agreements with Entities Whether the Accounts Are Held

Though SigFig understands and agrees with the NASAA's concern that the client's sharing of the credentials to their accounts held at other institutions could cause the client to violate their own user agreements with that institution, there are a few nuances to consider. First, while many user agreements of financial institutions that host client online accounts put the responsibility for confidentiality of client's password(s) on the client and disclaim liability for the damages resulting from client's decision to disclose these password(s), these agreements do not claim that the client's sharing of the password(s) constitutes a breach of contract. Additionally, despite the disclaimer, such financial institutions continue to provide fraud protection services and reserve the right to terminate client's online access in the event they have reason to believe that the security of the account password may be or has been compromised. An investment adviser who accepts the client's username and password subject to well-established cybersecurity and privacy controls would not be in violation of fiduciary duty.

III. Benefits of the Adviser's Ability to Access Client Accounts in Real Time

Finally, when suggesting the Proposed Rule Amendment, the NASAA did not consider the benefits that the advisers' access to client account information provides to both investors and advisers. A specific example is aggregation technology provided by digital wealth managers (or robo-advisors, as they are commonly known). This technology allows investors to link their financial accounts to one online platform, seeing holistic information in a single place, track balances, spending, receive real-time transactional data (which promotes fraud prevention, as the investor may more quickly detect unrecognized transactions when viewing everything in one place versus logging into different online accounts), and, in certain cases, receive useful analysis of their current portfolio holdings or overall financial situation. Advisers, in turn, use access to the linked client accounts to review their client's financial condition holistically, develop a thorough analysis, and ensure their recommendations are suitable and in the client's best interests. Our stance is that these benefits should be taken into account prior to restricting the practice of accessing client accounts with their credentials.

IV. Conclusion

SigFig agrees with the NASAA that the investment advisers' practice to access client accounts using client identifying information, such as username and password, gives rise to a number of concerns. However, we believe that the identified concerns can be addressed within the existing regulatory framework and, therefore, do not warrant an explicit prohibition of such practice.

SigFig supports the NASAA's goals and the importance of ensuring that clients' interests are protected. We appreciate the opportunity to provide our views regarding certain aspects of the Proposed Rule Amendment, and are welcoming an opportunity to discuss our comments with the Association. Please do not hesitate to contact me if we may provide additional information or clarification regarding the matters discussed herein.

Respectfully submitted,

Katrina Iamscicova
Counsel, Chief Compliance Officer