Q&As REGARDING THE ACCOUNT ACCESS AMENDMENT TO THE INVESTMENT ADVISER MODEL RULE ON UNETHICAL BUSINESS PRACTICES OF INVESTMENT ADVISERS AND INVESTMENT ADVISER REPRESENTATIVES

On May 19, 2019, the North American Securities Administrators Association, Inc. ("NASAA") adopted an amendment to NASAA's Unethical Business Practices of Investment Advisers, Investment Adviser Representatives, and Federal Covered Advisers Model Rule to prohibit investment advisers from accessing clients' electronic accounts through the clients' own unique identifying information (the "Account Access Model Rule").[1] The following Q&As are intended to help investment advisers understand the Account Access Model Rule, its purpose, and its application.

Q1: What conduct, act, practice, or course of business is NASAA addressing with the Account Access Model Rule?

A1: The Account Access Model Rule prohibits investment advisers from accessing client accounts using the client's own unique identifying log-in information (such as the client's username and password). The Account Access Model Rule does not apply to investment advisers that have received authorization from clients to access clients' electronic accounts through the investment adviser's own, unique log-in information (though there may be additional regulatory considerations for investment advisers in such circumstances, such as custody and recordkeeping issues).

Q2: Why did NASAA adopt the Account Access Model Rule?

A2: When an investment adviser accesses a client's account with the client's own unique log-in, the investment adviser is in effect impersonating this client and has the same access to the account as the client. This conduct raises multiple regulatory concerns, including, but not limited to, cybersecurity risks, possible violation of the client's user agreement and fraud protection policies with the electronic platform provider, custody concerns, and recordkeeping problems.

Q3: How do custody and the custody rule(s) factor into the Account Access Model Rule?

A3: Custody is often the first compliance issue that both regulators and investment advisers think of when exploring this issue. However, the NASAA model custody rule, Custody Requirements for Investment Advisers,[2] does not address all the issues implicated by this practice. Analyzing the extent to which an investment adviser's access to a client's account constitutes custody requires a consideration of many factors. Ultimately, such access generally will rise to the level of having custody if the investment adviser has any authority to obtain possession of (or the ability to appropriate) client funds or securities. Likewise, there is no easy way for a client, investment adviser, custodian, or regulator to distinguish

[1] Available at: http://nasaa.cdn.s3.amazonaws.com/wp-content/uploads/2011/07/1956-Unethical-Practices-Rule-Amended.pdf.

[2] Available at: http://www.nasaa.org/wp-content/uploads/2011/07/IA-Model-Rule-Custody.pdf.

between log-ins initiated by the investment adviser versus by the client (whether for recordkeeping or transactional purposes or after a suspected theft or fraud) if the investment adviser is using the client's username and password. The NASAA model custody rule pre-dates the extensive prevalence of this practice; the Account Access Model Rule supplements NASAA's model custody rule and provides additional investor protections.

Q4: What cybersecurity and user agreement/fraud protection concerns factored into the Account Access Model Rule?

A4: In addition to custody and recordkeeping issues, another concern is that this type of access may cause clients to violate their own user agreements with the electronic platform or website provider, potentially voiding certain contractual rights or account fraud protections and in turn creating potential liabilities. It is a common cybersecurity measure for user agreements to prohibit clients from providing another person with the client's username and password. Cybersecurity policies often provide some fraud protection but require that the client take reasonable steps to safeguard the client's username and password. If a client shares his or her log-in information with an investment adviser and suffers a loss in the account, the custodian may be able to disclaim liability it otherwise would have had pursuant to the client's user agreement. An investment adviser should not use a client's username and password if doing so could result in the client forfeiting protections otherwise provided by a custodian or expose the client to potential liability for breaching an account agreement. Investment advisers' fiduciary duties demand better for their clients.

Finally, in our age of cyber-threats, people should not as a general rule be giving *anyone* else their usernames and passwords. Investment advisers should not encourage clients to violate this fundamental cybersecurity principle.

Q5: I'm an investment adviser and my clients have authorized me to have read-only, third party access to view their accounts. Will the Account Access Model Rule affect me if it is adopted in the state(s) in which I conduct business?

A5: No, provided you are using your own unique log-in information. The Account Access Model Rule is targeted at *how* investment advisers access their clients' online accounts, not the scope of functionality investment advisers are authorized to have on behalf of their clients. However, keep in mind that there may be other issues (such as custody and record-keeping, both yours and the custodian's) even if you have your own unique identifying log-in information.

Q6: Does the Account Access Model Rule prohibit an investment adviser's use of data/account aggregation software?

A6: It depends on the data/account aggregation software, as the functionality of this software can differ among vendors. The Account Access Model Rule does not apply to an investment adviser's use of data/account aggregation software provided: (a) the investment adviser does not know, or have access to, the client's password(s); (b) there is an agreement between the data aggregation software company and the custodian(s)/online account

platform(s) to permit such back-door access to the client's account for data-aggregation purposes; and (c) access is entirely read-only, *i.e.,* the investment adviser can view information but cannot effectuate changes to the client's underlying account(s) through the data-aggregator.

Q7: Has my jurisdiction adopted the Account Access Model Rule?

A7: Check with your state securities regulator to determine whether the Account Access Model Rule has been implemented in your state. In addition, please be mindful that your state securities regulator may have enacted other rules in regard to this (and other) investment advisory practices. It is therefore a good practice to keep abreast of all regulatory changes affecting your business.[3]

Q8: I am an investment adviser and currently access at least one client's account with the client's own unique identifying log-in information (username and password). What should I do now?

A8: First off, take steps to ensure you are complying with your regulatory and other legal requirements. Discuss this issue with your own private legal counsel. Contact your regulator(s) directly. Additionally, contact the respective custodians or platform providers and request they provide you with your own unique log-in information. If your custodian objects or professes inability to do this, consider potential alternative arrangements (such as switching custodians or arranging for direct delivery of client account statements to you). Again, reach out to your regulator(s) if you encounter any additional issues.

Q9: Who can I contact if I have questions about the Account Access Model Rule?

A9: Please contact the NASAA Corporate Office's Legal Department, at 202-737-0900.

Q&A Publication Date: December 1, 2017

[3] Contact information for NASAA members is available at: http://www.nasaa.org/about-us/contact-us/contact-your-regulator/.