



**FINANCIAL
SERVICES
INSTITUTE**

VOICE OF INDEPENDENT
FINANCIAL SERVICES
FIRMS AND INDEPENDENT
FINANCIAL ADVISORS

VIA ELECTRONIC MAIL

April 11, 2021

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

Re: Release No. 33-11028; File No. S7-04-22
Cybersecurity Risk Management Rules for Investment Advisers, Registered Investment
Companies, and Business Development Companies

Dear Secretary Countryman:

On February 9, 2022, the Securities and Exchange Commission (SEC) published its request for public comment on proposed recommendations to Cybersecurity Risk Management Rules for Investment Advisers, Registered Investment Companies, and Business Development Companies (Proposed Rules, collectively, the Proposal).¹ The SEC's goal for the Proposal is to bolster its efforts to protect investors, market participants, and the financial services industry from cyberattacks that have increased in recent years.

The Financial Services Institute² (FSI) appreciates the opportunity to comment on this important proposal which will impact FSI members specifically and the financial services industry as a whole.³ FSI and its members believe there is common interest in establishing effective and sensible practices to protect firms and the investing public from cybersecurity threats. Any cybersecurity framework promulgated by the SEC should provide flexibility for financial industry participants to exercise their judgment and experience to adopt and adjust effective cybersecurity practices. While we support the Proposal as a whole, we do provide selected comments on cybersecurity incident reporting and other aspects of the Proposal to help streamline its application and maximize the impact investment advisers can have towards this common interest of protecting firms and the investing public from cyberattacks.

¹ Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (proposed March 9, 2022).

² The Financial Services Institute (FSI) is an advocacy association comprised of members from the independent financial services industry, and is the only organization advocating solely on behalf of independent financial advisors and independent financial services firms. Since 2004, through advocacy, education and public awareness, FSI has been working to create a healthier regulatory environment for these members so they can provide affordable, objective financial advice to hard-working Main Street Americans.

³ We note that while the Proposal also includes investment companies and business development companies, we have focused our comments solely on the investment adviser component of the Proposal. All references to the Proposal and Proposed Rules focus on Advisers Act rules.

Background on FSI Members

The independent financial services community has been an important and active part of the lives of American investors for more than 40 years. In the US, there are more than 160,000 independent financial advisors, which account for approximately 52.7 percent of all producing registered representatives.⁴ These financial advisors are self-employed independent contractors, rather than employees of the Independent Broker-Dealers (IBD).⁵

FSI's IBD member firms provide business support to independent financial advisors in addition to supervising their business practices and arranging for the execution and clearing of customer transactions. Independent financial advisors are small-business owners and job creators with strong ties to their communities. These financial advisors provide comprehensive and affordable financial services that help millions of individuals, families, small businesses, associations, organizations, and retirement plans. Their services include financial education, planning, implementation, and investment monitoring. Due to their unique business model, FSI member firms and their affiliated financial advisors are especially well positioned to provide Main Street Americans with the affordable financial advice, products, and services necessary to achieve their investment goals.

FSI members make substantial contributions to our nation's economy. According to Oxford Economics, FSI members nationwide generate \$35.7 billion in economic activity. This activity, in turn, supports 408,743 jobs including direct employees, those employed in the FSI supply chain, and those supported in the broader economy. In addition, FSI members contribute nearly \$7.2 billion annually to federal, state, and local government taxes.⁶

Discussion

FSI appreciates the opportunity to comment on the SEC's Proposal with a focus on selected provisions. As we note below, we believe the financial services industry as a whole, including FSI and its members, share a common interest in protecting firms and the investing public from cybersecurity threats. We offer our comments, discussed in greater detail below, with the goal to streamline certain of the Proposal's aspects, align to other cybersecurity and data privacy regimes, and maximize the impact investment advisers can have towards this common interest of protecting firms and the investing public.

I. The SEC and Industry Participants Share a Common Interest in Establishing Effective and Sensible Practices to Protect Firms and the Investing Public from Cybersecurity Threats

A. Introduction

FSI members (whether firms or individual advisors) have a common interest with the SEC to ensure effective and sensible practices to protect the financial industry and the investing public

⁴ Cerulli Associates, Advisor Headcount 2016, on file with author.

⁵ The use of the term "financial advisor" or "advisor" in this letter is a reference to an individual who is a registered representative of a broker-dealer, an investment adviser representative of a registered investment adviser firm, or a dual registrant. The use of the term "investment adviser" or "advisor" in this letter is a reference to a firm or individual registered with the SEC or state securities division as an investment adviser.

⁶ Oxford Economics for the Financial Services Institute, The Economic Impact of FSI's Members (2020).

from cybersecurity threats. Effective cybersecurity protection in turn calls for collaboration between the financial industry (including FSI and its membership) and the SEC. Furthermore, as cybersecurity practices are inherently technology-driven, the financial industry has and continues to play a key role in developing and identifying new technology and methods to address ever-evolving cybersecurity threats. The financial industry has already developed workable and effective practices in response to cybersecurity requirements generally aligned with state laws and regulations⁷ and the General Data Protection Regulation (GDPR).⁸ At the state level, harmonization with existing financial industry cybersecurity regulations is evidenced by the exemption of entities subject to the Gramm-Leach-Bliley Act.⁹ While both U.S. state-level privacy requirements and GDPR requirements have certain drawbacks,¹⁰ they have impacted a significant portion of the investment adviser industry, including FSI members, and we urge the SEC to consider uniformity as much as possible while incorporating input through this comment process.

B. FSI Agrees with the General Framework of the Proposal, but Provides Comments to Several Areas to Ensure Increased SEC-Industry Collaboration

FSI notes that the Proposal relies on four key components, addressing disclosure, reporting and policies and procedures:

- Investment adviser cybersecurity policies and procedures that address risk assessment, user security and access, information protection, cybersecurity threat and vulnerability management and incident response and recovery;
- Investment advisers report to the SEC within 48 hours of a significant cybersecurity incident, with a requirement that the adviser amend any report promptly after any information becomes materially inaccurate and/or new information is uncovered and/or resolution occurs;
- Form ADV disclosures for investment advisers to describe material cybersecurity risks, which advisers must promptly amend and re-deliver to clients if there are material revisions; and
- A recordkeeping requirement documenting the above and related items.

These four components provide a framework to achieve the SEC's outlined goals, but the Proposal should be designed to allow for more flexibility than is currently provided. Considering the complexity and the inter-connectivity in the financial industry, FSI appreciates that cybersecurity failure by one segment can potentially affect other segments of the industry. As such, FSI generally does not object to thoughtful regulatory requirements regarding cybersecurity, particularly when, as with sound policies and procedures, such requirements build on existing industry best practices.

⁷ See e.g. California Consumer Privacy Act (CCPA) Cal. Civ. Code §1798.100 et seq; Virginia Consumer Data Protection Act (CDPA) Va. Code §59.1-571 et seq.

⁸ Appropriate technical and organizational measures must be used given the nature and sensitivity of personal data involved, General Data Protection Regulation (GDPR) Art. 25.

⁹ CDPA § 59.1-572(B)

¹⁰ See e.g. GDPR cross border data flow issues - invalidation of Privacy Shield, Schrems II decision and subsequent European Data Protection Board guidance regarding cross border transfer requirements.

C. FSI Believes that the SEC Should Take into Account Cybersecurity Requirements Already Applicable or Applied to Investment Advisers

FSI appreciates that the SEC's Proposal is focused on investment advisers partially as a result of a concern that some advisers have not implemented reasonably designed cybersecurity programs.¹¹ FSI notes, however, that a significant subset of SEC-registered investment advisers are not standalone businesses, but rather affiliated or dually registered with broker-dealers. Broker-dealers are subject to FINRA-specific cybersecurity requirements.¹² Therefore, investment advisers affiliated with or dually registered with broker-dealers already are under the ambit of enterprise-wide, financial services focused, cybersecurity compliance programs. The majority of FSI member firms have structures that include both broker-dealers and investment advisers.

Furthermore, investment advisers, like broker-dealers, must remain in compliance with Reg S-P¹³ and Reg S-ID.¹⁴ Reg S-P requires advisers (as well as broker-dealers and investment companies) to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information, pursuant to several parameters. Reg S-ID programs must include reasonable policies and procedures to identify and detect relevant red flags, as well as respond appropriately to red flags so as to prevent and mitigate identity theft. Maintaining this type of uniformity in obligations for investment advisers and broker-dealers is beneficial.

Beyond the realm of existing SEC and FINRA requirements, SEC-registered investment advisers can be part of larger financial services companies, including banks. In those instances, enterprise level compliance with existing cybersecurity best practices as well as information sharing through other systemic regulatory bodies (e.g. Financial Services Information Sharing and Analysis Center ("FS-ISAC")) are generally also extended to investment advisers.

In light of the relative maturity of other financial services' cybersecurity requirements, we urge the SEC to consider aligning cybersecurity requirements for investment advisers more closely to existing requirements for other financial institutions. This would contribute to ensuring a significant level of uniformity across an enterprise, comprising of one or several investment advisers, as opposed to placing requirements solely on investment advisers, particularly if such requirements differ from affiliated financial services providers.

II. The SEC should Balance a Prompt Cybersecurity Incident Reporting Requirement with the Uncertain Nature of Initial Fact Finding Immediately After an Incident

A. Introduction

As the Proposal is currently drafted, advisers would notify the Commission of *significant* adviser/fund cybersecurity incidents through a new electronic Form ADV-C on the Investment Adviser Registration Depository (IARD) no more than 48 hours after having a "reasonable basis to

¹¹ Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524, 13527 (proposed March 9, 2022).

¹² FINRA Rules § 3110 Supervision; § 3120 Supervisory Control Systems; § 4530(b) Reporting Requirements.

¹³ SEC Regulations S-P, S-AM, and S-ID, 17 C.F.R. § 248.1-248.31 (2022).

¹⁴ SEC Rules of Practice, 17 C.F.R. § 201 (2022); SEC Informal and Other Procedures, 17 C.F.R. § 202 (2022).

conclude that any such incident has occurred or is occurring.”¹⁵ FSI seeks a thoughtful dialogue on this issue, as the Form ADV-C requirement, as currently written, remains challenging and possibly wholly unworkable for investment advisers to file at the levels of specificity and accuracy expected within 48 hours. FSI notes that the Proposal does not contemplate a safe harbor for investment adviser registrants who would be required to file Form ADV-C multiple times as they gather information and findings evolve and change with additional information.

In addition to the 48 hour requirement for an initial filing of Form ADV-C, the Proposal would require advisers to amend any Form ADV-C reports promptly, but in no event more than 48 hours after at least one of three conditions is met. These conditions are (1) after information reported on the Form in the past has become materially inaccurate, or (2) after new material information about a previously reported incident is uncovered, or (3) resolving a previously reported incident or closing an internal investigation to a previously disclosed incident.

B. FSI Recommends the SEC Reconsider the Timing, Breadth and Scope of the Proposed Form ADV-C Requirement

FSI notes that, in practice, the Form ADV-C filing schedule applied to an active breach investigation could result in constantly changing updated filings for Form ADV-C and, until the investment adviser has further identified additional information regarding the incident, require an impractical level of specificity early on in a cyber incident.

Notwithstanding reservations regarding Form ADV-C, the Proposal’s threshold for reporting a Significant Cybersecurity Incident generally aligns with other privacy law regimes.¹⁶ FSI commends the SEC for drawing from existing privacy and reporting regimes and recommends considering the timing and scope of other regimes. This could include drawing from one of the following existing or proposed reporting requirements:

- SEC’s 4-day proposed requirement for public companies¹⁷
- GDPR’s 72 hour notification of a personal data breach to the supervisory authority¹⁸

If the final rule includes a 48 hour reporting requirement, FSI recommends the SEC streamline the initial report to be less detailed than Form ADV-C and not to require additional reports until completion of the internal investigation or 30 days after the initial report, whichever date is sooner. If completion of the internal investigation does not occur at 30 days, the SEC could require a third report at conclusion of the internal investigation.

FSI recommends that an initial Form ADV-C only contain questions (1)-(5) and (7), with an abbreviated question (6) that only includes the first question of 6, but not (6)(a) or (6)(b). This

¹⁵ Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524, 13537 (proposed March 9, 2022).

¹⁶ See e.g. HIPAA Breach Notification Rule 45 CFR § 164.400 et seq.

¹⁷ See Press Release, SEC, SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (March 9, 2022), <https://www.sec.gov/news/press-release/2022-39>; Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590 (proposed March 9, 2022).

¹⁸ Note that GDPR allows for time to understand if the incident rises to the level of reportable breach. General Data Protection Regulation (GDPR), OJ 2016 L 199/1, at 33(1), available at <https://gdprinfo.eu/>.

would further align the initial report with limited scope reporting in other data privacy and reporting regimes and lessen the burden of reporting on an accelerated timeframe such as 48 hours. FSI also recommends that the SEC consider further uniformity with reporting regimes as Form ADV-C, as currently drafted, is designed to elicit a granular level of detail that may further compromise an investment adviser, should Form ADV-C information become available more widely.

C. FSI Urges Additional Clarity on the Confidentiality of Form ADV-C

FSI understands and appreciates the importance of transparency and information sharing in the context of reportable events and supports Form ADV-C being confidential. However, investment advisers may be asked to waive confidentiality of Form ADV-C in situations such as due diligence. FSI asks that the SEC clarify that Form ADV-C is confidential and for regulator use only as part of any final rulemaking and include this clarification in Rule 204-6.

D. FSI Urges Additional Safe Harbor Provisions for Form ADV-C

FSI notes the potentially chilling effect of Form ADV-C, as currently drafted, for investment advisers, especially those with a smaller staff. An investment adviser would be filing Form ADV-C during a time when resources are best used to abate the attempted intrusion(s) of a bad actor seeking to victimize an investment adviser. Investment advisers would make the Form ADV-C filing based on accurate facts known at the time, but events and information may be fast moving and subject to change upon further investigation. Safe harbor language would provide additional SEC acknowledgement that the information advisers submit may evolve. Safe harbor language could be included in the preamble of the Proposal's Rule 204-6, noting that all but the final filing of a Form ADV-C provides a non-exclusive safe harbor from compliance with Rule 204-6 and 206(4)-9.

III. FSI Provides Additional Comment on Disclosures, Risk Assessment and Technical Requirements

A. Introduction

The Proposal also includes other requirements for risk assessments and certain technical requirements. We offer below narrow, targeted comments.

B. Form ADV Part 2A Disclosures

FSI recommends that any Form ADV Part 2A disclosures regarding cybersecurity and incidents be limited to an annual amendment, rather than the promptness requirement currently part of the Proposal. FSI notes that the Proposal's scope of Form ADV 2A disclosures regarding cybersecurity risk will not allow for meaningful comparison across investment advisers, as all firms face a certain amount of common risks. Furthermore, with regard to using Form ADV 2A as an additional vehicle for incident reporting, FSI notes that any clients affected by an incident would receive notification pursuant to state law and that multiple mailings of Form ADV Part 2A to investors to disclose any incidents would be duplicative and not trigger client engagement. FSI also recommends not over-expanding Form ADV 2A, which has already become an extensive and lengthy document for most investment advisers.

C. Risk assessment

FSI appreciates the Proposal including a risk assessment requirement and notes that such assessments are already part of existing cybersecurity programs within the financial services industry. We offer two comments for consideration:

1. Uniformity in criteria – Requiring investment advisers to evaluate or assess vendors on a set of criteria can be helpful if a uniform assessment template or roadmap is provided. Otherwise, if investment advisers are evaluating vendors on different criteria, the underlying policy reason for this requirement (robust third-party risk assessments) would be diluted. There are existing risk assessment frameworks¹⁹ that the SEC could leverage to make this aspect of the Proposal both more workable and robust.

2. Acknowledge differences in vendors – Performing a risk assessment of a large, established technology vendor (e.g. Amazon Web Services, Microsoft Azure) will have different inputs than for other vendors, and investment advisers may have less negotiating ability. FSI notes that uniformity in criteria may even such differences.

D. Technical Requirements

FSI notes that the Proposal also addresses various technical requirements in the rule, such as multi-factor authentication (MFA). Such technical requirements will likely become stale in the next 1-5 years, if not sooner. FSI proposes that the SEC identify MFAs and other specific practices as current examples as opposed to evergreen requirements and leverage additional existing frameworks. In the alternative, the SEC could ensure staff provides updated FAQs or otherwise update such requirements in a transparent manner accessible to investment advisers.

IV. The SEC Should Consider Including Mechanisms in The Proposal to Ensure Transparency as Best Practices Evolve to Address Technological Changes and Threats

As noted above, the on-the-ground cybersecurity protection experience of the financial services industry, including FSI members, is critical to the ongoing development of effective cybersecurity practices. In the final rule release amending and adopting the Proposal, we recommend the SEC affirmatively commit to agency best practices that are updated on a regular basis. Such best practices should include financial industry input, through consultation and collaboration, given the rapidly evolving nature of technology and, in many cases, also the tactics utilized by bad actors. For instance, the SEC should affirmatively commit to solicitation of input from the industry to provide periodic FAQs and guidance. Such guidance will allow for investment advisers to continue to pro-actively protect information and follow best practices, which is better from an investor protection standpoint than if the SEC were to use enforcement to set standards. In addition, the SEC should commit to avoiding using enforcement to set standards, which could be further demonstrated through safe harbor language and regular FAQs, as mentioned above.

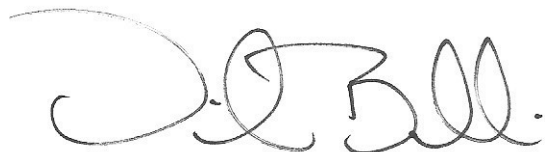
¹⁹ Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5; Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC 27001. Both are widely relied upon in developing sectoral and omnibus data privacy and security regulations.

Conclusion

We are committed to constructive engagement in the regulatory process and welcome the opportunity to work with the SEC on this and other important regulatory efforts.

Thank you for considering FSI's comments. Should you have any questions, please contact me at [REDACTED].

Respectfully submitted,

A handwritten signature in black ink, appearing to read "D. T. Bellaire". The signature is fluid and cursive, with a large initial "D" and "T" followed by the name "Bellaire".

David T. Bellaire, Esq.
Executive Vice President & General Counsel