

June 12, 2023

Ms. Vanessa Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC, 20549-1090

Re: Supplemental Comments of the
Investment Company Institute on File No.
S7-06-23 (Cybersecurity Risk Management
for Broker-Dealers et al.); File No. S7-05-23
(Proposed Revisions to Regulation S-P); and
File No. S7-04-22 (Cybersecurity Risk
Management for Investment Advisers et. al.)

Dear Ms. Countryman:

In the April *Commission Statement Relating to Certain Administrative Adjudications*¹ and the *Second Commission Statement Relating to Certain Administrative Adjudications*,² the Securities and Exchange Commission (Commission or SEC) announced that there had been an ongoing internal breach by the SEC's Division of Enforcement of the databases maintained by the Commission's Office of the Secretary.³ The substance of the Second Statement and its five exhibits were succinctly summarized in a June 5, 2023 *Ignites* article entitled "SEC Dismisses 42 Cases Compromised by Firewall Breach."⁴ On June 7, 2023, there was another *Ignites* article

¹ <https://www.sec.gov/news/statement/commission-statement-relating-certain-administrative-adjudications>.

² <https://www.sec.gov/news/statement/second-commission-statement-relating-certain-administrative-adjudications>.

³ Notwithstanding the Commission's recent lengthy Statement regarding these breaches, the Statement does not provide important details about the breach, including how long this has been going on. It appears from the information provided, however, that the system may have been breached as early as 2015 – eight years without being detected.

⁴ See article by Joe Morris dated June 5, 2023, available at:
https://www.ignites.com/c/4097814/526914?referrer_module=searchSubFromIG&highlight=firewall

that described a ransomware attack of Casepoint, a vendor utilized by the Commission to handle “troves of sensitive documents.” The article indicated that the SEC declined to comment regarding the ransomware attack and Commission information that may have been compromised as a result of the attack.⁵

In light of these Commission Statements and disclosure of the Casepoint attack, the Investment Company Institute is writing to supplement the comments we previously submitted to the Commission on its proposals to: require broker-dealers and transfer agents to have cybersecurity risk management programs; revise Regulation S-P to require breach notices; and to require registered investment companies and investment advisers to have cybersecurity risk management programs. The comment we previously submitted to the Commission on these proposals discussed the Commission’s information security challenges that, unfortunately, are not new. Indeed, as detailed in our comment letters,⁶ there is more than a decade of audits documenting the inadequacy of the Commission’s information security. These audits raise important questions about, and highlight serious concerns with, the SEC’s information security environment. We do not believe that the Commission would tolerate any SEC registrant having a similar history documenting the inadequacy of their information security controls.

In part, the Commission’s rule proposals would require registrants to submit to the Commission highly sensitive information regarding any significant cybersecurity incidents. In our comment letters, we opposed the Commission collecting this information due to our concerns with the SEC’s inability to ensure the protection of its information.

Considering the recent internal breach and compromise of the Commission’s systems and non-public information, our concerns with the vulnerability of registrants’ information held by the Commission are even greater. Until audits of the Commission’s information security systems document that the Commission’s security is “effective” in all aspects, we urge the Commission not to proceed with its proposals to collect any sensitive information regarding registrants’ cybersecurity incidents.

We also reiterate our recommendation that the Commission adopt rules requiring it to promptly notify impacted persons whenever the Commission (or a service provider to the Commission) experiences a breach of its systems. Providing breach notifications is critical to helping registrants and others take steps necessary to protect their interests and the interests of their investors and clients from the harm that may flow from such breach.

⁵ See article by Beagan Wilcox Volz dated June 7, 2023 available at: https://www.ignites.com/c/4102214/527174?referrer_module=searchSubFromIG&highlight=hackers

⁶ ICI Comment Letter on Cybersecurity Risk Management for Broker-Dealers et. al. (May 23, 2023), available at <https://www.ici.org/system/files/2023-05/23-cl-sec-cyber-proposal.pdf>; ICI Comment Letter on proposed changes to Regulation S-P (May 23, 2023), available at: <https://www.ici.org/system/files/2023-05/23-cl-sec-reg-sp-proposal.pdf> and ICI Comment Letter on Cybersecurity Risk Management for Investment Advisers et. al. (May 22, 2023 and April 11, 2022), available at <https://www.ici.org/system/files/2023-05/23-cl-sec-cyber-reproposal.pdf>, and <https://www.sec.gov/comments/s7-04-22/s70422-20123076-279408.pdf>.

Sincerely,

A handwritten signature in cursive script, appearing to read "Susan M. Olson".

Susan Olson
General Counsel
Investment Company Institute

cc: Gary Gensler, Chair, Securities and Exchange Commission
Hester M. Peirce, Commissioner, Securities and Exchange Commission
Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission
Mark T. Uyeda, Commissioner, Securities and Exchange Commission
Jaime Lizárraga, Commissioner, Securities and Exchange Commission