DODGE & COX

Investment Managers

October 31, 2017

Mr. Jay Clayton
Chairman, U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-9303

Re: Investment Company Reporting Modernization – File Nos. S7-08-15

Dodge & Cox respectfully submits this letter in response to your recent Statement on Cybersecurity, published on September 20, 2017. We appreciate your speaking out about this important issue and agree with your assessment that cyber threats pose an increasing risk to our financial systems and markets, and that the Securities and Exchange Commission is and will continue to be a target for cyber criminals. In light of this risk, we wish to reiterate the concerns expressed in our August 7, 2015 comment letter[1] regarding the Investment Company Reporting Modernization Rule and ask that the Commission reconsider limiting the Form N-PORT reporting requirement in the rule to public quarterly filings. If the Commission continues to believe that monthly portfolio holdings reports are necessary, we ask that it adopt a quarterly filing requirement that includes monthly position data on a delayed basis.

We believe the risk that investment company monthly portfolio holdings data could be stolen and used for predatory trading activities is significant. In your statement, you acknowledge that the SEC is a frequent target of cyber attacks and that at least one such successful attack against the SEC last year may have been used to misappropriate non-public information given to the Commission in its regulatory capacity. A recent report by the U.S. Government Accountability Office concluded that, while the SEC has improved its security controls, substantial deficiencies remain, including a lack of consistent protection of its network boundaries from possible intrusions.[2] Indeed, the SEC's own Office of Inspector General concluded recently that the SEC's information security program did not meet the standards established by the Federal Information Security Modernization Act of 2014 ("FISMA"); in particular, it noted that the SEC does not have an effective information security continuous monitoring program, enabling it even to identify network intrusions.[3]

---

[1] Dodge & Cox Funds, Comment Letter in respect of the Proposing Release Nos 33-9776; 34-75002; IC-31610: Investment Company Reporting Modernization, August 7, 2015, www.sec.gov/comments/s7-08-15/s70815-200.pdf ("Dodge & Cox Comment Letter").
[2] SEC Improved Control of Financial Systems but Needs to Take Additional Action, Highlights of GAO-17-469, a report to the Chair, U.S. Securities and Exchange Commission, July, 2017.
[3] Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2016, U.S. Securities and Exchange Commission Office of Inspector General, Office of Audits, March 7, 2017.

While we applaud the Commission's efforts to improve cyber security systems at the SEC and to encourage sound cyber risk management practices throughout the financial system, we note that the SEC routinely faces budgetary constraints that are certain to hinder its efforts to build and maintain a robust cyber security program. Further, it is generally accepted that even the most diligent cyber security efforts cannot thwart all attacks. Cyber attacks have been successful in recent years against many private and public institutions with state-of-the-art cyber security programs.[4] Regrettably, it seems likely that, no matter how sophisticated the Commission's defenses, more attacks will succeed in the future, particularly if state actors decide to focus on disrupting U.S. markets.

We understand the Commission's desire for more detailed information about investment company portfolio holdings presented in a format that facilitates analysis across entities. However, we believe the risk of misappropriation of confidential monthly portfolio holdings reports covering the entire investment company industry outweighs the potential usefulness to the Commission of collecting and storing this information. Clearly, a warehouse of non-public industry-wide monthly portfolio holdings in an easily exploitable structured data format creates a rich target for cyber criminals that could potentially be used to the detriment of the very investors the Commission seeks to protect. As explained in our prior comment letter (see attached), academic studies and our own analysis suggests that even the public disclosure of portfolio holdings under the existing Form N-Q has provided the basis for predatory trading, permitting front-running, as well as free-riding off the research and portfolio management skills of mutual fund investment advisors and hurting investor returns.[5] Retail shareholders, whose only access to high quality investment management services is typically through mutual funds, are impacted disproportionately by these sorts of predatory trading behaviors.

Given the risk of harm to investors if industry-wide portfolio holdings information were stolen and misused, the Commission should be conservative with respect to the volume and type of non-public market information it proposes to collect and store, particularly given its inability to guarantee the security of that information. In the Proposing and Adopting Releases for the Investment Company Reporting Modernization Act, the Commission argues that monthly portfolio reporting will be useful to the staff for monitoring funds, particularly during periods of market stress and will better enable the staff to monitor for industry trends.[6] However, beyond a general assertion that more data is better, neither Release articulates a specific need or compelling justification for more frequent reporting; in

---

[4] For example, JP Morgan, Anthem, Equifax, and other major companies have suffered major data breaches in the past few years. See, e.g., "JPMorgan and Other Banks Struck by Hackers," The New York Times, August 27, 2014; "Millions of Anthem Customers Targeted in Cyberattack," The New York Times, February 5, 2015; "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," The New York Times, September 7, 2017. Recent U.S. government data breaches have included the Internal Revenue Service ("Cyberattack Exposes I.R.S. Tax Returns," The New York Times, May 26, 2015), Office of Personnel Management ("Hacking of Government Computers Exposed 21.5 Million People," The New York Times, July 9, 2015, and even the National Security Agency ("New N.S.A. Breach Linked to Popular Russian Antivirus Software," The New York Times, October 5, 2017 and, allegedly, the CIA ("WikiLeaks says it has obtained trove of CIA hacking tools," The Washington Post, March 7, 2017.

[5] See Dodge & Cox Comment Letter, pp 2-5.

[6] Investment Company Reporting Modernization, 17 CFR Parts 200, 210, 232, 239, 240, 249, 270, 274, Final Rule Release; October 3, 2016, www.sec.gov/rules/final/2016/33-10231.pdf, p. 140-141.

particular, no claim is made that more frequent reports are needed in order for the Commission to enforce existing regulations.

Finally, in addition to the harm to investors and asset managers, the SEC should consider the risk to its own reputation from a cyber attack on the SEC's database resulting in the misappropriation and misuse of valuable proprietary information. If it hasn't already done so, we suggest that the SEC undertake a thorough analysis of the risks and rewards to the agency when considering reporting requirements involving sensitive information. Dodge & Cox believes that effective regulation is essential to the health and success of the financial services industry and capital markets, but that the SEC's zeal to collect more and more information could backfire, damaging its mission and standing. A breach would at best be an embarrassing distraction to the SEC and at worst could weaken public and political support and lead to diminishment of its role.

In our letter, we proposed that the Commission collect monthly portfolio holdings data, but on a quarterly basis, subject to a 60-day delay. This would give the Commission the more detailed data needed to conduct additional analysis as to market and industry trends, without the risk of exposing nearly-current holdings information. We urge the SEC to carefully reconsider the benefits relative to the risks of its collection of fund portfolio holding information on a monthly basis, and submit that the agency can reduce those risks while still achieving its regulatory goals with quarterly reporting. We appreciate your consideration of our concerns and would welcome the opportunity to discuss this matter further. Please contact Roberta R.W. Kameda, General Counsel, with any questions about this letter.

Very truly yours,

Charles F. Pohl
Chairman and Chief Investment Officer
Dodge & Cox