Statement

Statement on Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Commissioner Allison Herren Lee

Feb. 9, 2022

Cyber-attacks have increased at an alarming rate in recent years in terms of size, frequency and sophistication. The Equifax breach in 2017 could cost the company as much as $700 million, and affected over 145 million consumers.[1] In 2019, SolarWinds experienced a major cyber breach that impacted nearly 18,000 of its customers, prompting the U.S. Department of Homeland Security to issue an emergency directive to all federal agencies.[2] The acceleration has continued unabated into 2021 with the Colonial Pipeline Company becoming the victim of an attack that heavily disrupted the flow of gas to the East Coast for days,[3] and one of the largest U.S. insurance companies reportedly paying $40 million to hackers after it suffered a ransomware attack.[4] In fact by some measures, we've seen a more than a 68% increase since 2020 in the overall number of data compromises, [5] and a concomitant rise in the sophistication of these bad actors.[6]

Funds and their advisers, because of the data they store and manage, are enticing targets for such activity which can cause serious investor and market harm.[7] The proposal takes a much-needed holistic approach to the issue rather than the more discrete and piecemeal approach we've taken thus far.[8] Importantly, our efforts today acknowledge that cybersecurity threats can have a profound impact on the financial system, and establish the groundwork for a more collective and collaborative approach among a variety of parties including the adviser, the fund board, and others. This in turn will build transparency, responsiveness and accountability.

Today's release includes important investor protections designed to address cybersecurity risks in a comprehensive way. For instance, the proposal includes a requirement for advisers and funds to adopt and implement written cybersecurity policies and procedures.[9] This will help establish a first line of defense in protecting both firms and investors, and is just one of many ways the proposal would increase investor protection and market integrity.

Another key provision of the proposal is the notification to the Commission of certain cybersecurity incidents.[10] This will enhance our ability to monitor and help address cybersecurity incidents that could have potentially broader system-wide impacts.[11] These provisions raise a number of questions. For example, the proposal would require notification to the Commission of an incident within 48 hours, but the notification to an adviser's clients has

no specific timeframe. Instead such notification would need to be made "promptly." Should investor notification be tied to a more discrete timeframe to ensure timeliness? And, what specific information do investors need to know about such incidents?

I welcome the public's input on these and all other provisions in the proposal, as we work to develop a transparent, nimble and accountable framework for investment advisers and funds. I also very much look forward to the Commission staff's recommendation on cyber-related rules impacting issuers. I'm pleased to support this proposal, and I want to thank the staff in the Divisions of Investment Management and Economic Risk and Analysis, as well as the General Counsel's office.

---

[1] Press Release, Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related. *See also* Cybersecurity & Infrastructure Security Agency, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Oct. 26, 2020), at Appendix C and page 105, *available at* https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

[2] U.S. Department of Homeland Security Emergency Directive 21-01, Mitigate SolarWinds Orion Code Compromise (Dec. 13, 2020), *available at* https://cyber.dhs.gov/ed/21-01/. *See also* U.S. Government Accountability Office, SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic) (Apr. 22, 2021), *available at* https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[3] Press Release, Colonial, *Media Statement Update: Colonial Pipeline System Disruption* (last visited Feb. 8, 2022), *available at* https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption. *See also* Remarks by President Biden on the Colonial Pipeline Incident (May 13, 2021), *available at* https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.

[4] *CNA Security Incident Update* (Mar. 23, 2021), *available at* https://www.cna.com/web/wcm/connect/5588fffe-ed63-4e86-986d-22e81648ac21/CNA-Security-Incident-Update-March-23.pdf?MOD=AJPERES. *See also* Kartikay Mehrotra and William Turton, *CNA Financial Paid $40 Million in Ransom After March Cyberattack* (May 20, 2021), *available at* https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.

[5] Identify Theft Resource Center, *Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises* (Jan. 24, 2022), *available at* https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

[6] *See, e.g.*, Center for Strategic and International Studies, *Significant Cyber Incidents* (last visited Feb. 8, 2022), *available at* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; Cybersecurity & Infrastructure Security Agency, National Cyber Awareness System Alerts (last visited Feb. 8, 2022), *available at* https://www.cisa.gov/uscert/ncas/alerts.

[7] Press Release, U.S. Securities & Exchange Commission, SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (Aug. 30, 2021), *available at* https://www.sec.gov/news/press-release/2021-169 (sanctioning eight firms for failures in their cybersecurity policies and procedures).

[8] *See, e.g.,* Division of Investment Management Cybersecurity Guidance, IM Guidance Update No. 2015-02 (Apr. 2015), *available at* https://www.sec.gov/investment/im-guidance-2015-02.pdf; Division of Investment Management, Business Continuity Planning for Registered Investment Companies, IM Guidance Update No. 2016-04 (June

2016), *available at* https://www.sec.gov/investment/im-guidance-2016-04.pdf; Cybersecurity and Resiliency Observations, Office of Compliance Inspections and Examinations (Jan. 27, 2020), *available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf; Division of Examinations Cybersecurity Initiative (Apr. 15, 2014), *available at* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf; Division of Examinations 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), *available at* https://www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf.

[9] Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Securities Act of 1933 Release No. 33-11028 (Feb. 9, 2022).

[10] *Id.*

[11] As we've seen many times before, cybersecurity events can have broad economic impacts. *See, e.g.*, Center for Strategic and International Studies and McAfee, *Economic Impact of Cybercrime – No Slowing Down* (Feb. 2018), *available at* https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf, at 4 (stating that "cybercrime may now cost the world almost $600 billion" from $500 billion in 2014).