Statement

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

Commissioner Caroline A. Crenshaw

Feb. 9, 2022

The threat of cyberattacks on U.S. financial services firms is one of those issues that keeps me up at night. Financial services firms are leading targets of cyberattacks because "that's where the money is."[1] Cyberattacks don't just have the potential to disrupt individual firms and their immediate clients - they have the potential to cause market-wide instability. The G20 recently warned that cyberattacks could "disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability."[2]

Investment advisers and funds manage tens of trillions of investor dollars.[3] They can be targeted directly or indirectly through the web of service providers that many firms must use to conduct business.[4] The latter creates a broad array of potential exposure and their critical business functions can be adversely impacted in numerous ways.[5] These potential points of vulnerability include the loss of customer's personally identifiable information, the inability to access accounts or trade, the theft of intellectual property, confidential or proprietary information, or even the theft or loss of client assets.

Further, there has been an increase in the frequency and sophistication of cyberattacks[6]-- meaning a corresponding increase in risk to investors whose assets are held by the firms.

Given these realities, robust cyber hygiene practices are critical, both to safeguard investor money entrusted to firms and advisers and to guard against market-wide instability. Today's proposal would require all registered advisers and funds to design and implement cybersecurity policies and procedures in order to be prepared for future cyber threats. And such policies and procedures would be subject to recordkeeping requirements so that deficiencies can be identified and addressed.[7]

Additionally, investors need relevant information to inform their investment decisions. And this holds true when it comes to cybersecurity risks. Today's proposal would require advisers and funds to tell investors about the cybersecurity risks they anticipate, how they would handle those threats, and the nature and scope of any significant cybersecurity incidents that occurred in the past two years. Further, the proposal would require regulatory reporting of any significant cybersecurity incidents to the Commission within 48 hours, and prompt

notification to investors.[8] This would give the Commission data to assess trends, identify emerging risks, and help coordinate responses to cyber incidents that have the potential to cause broader disruptions, as well as providing investors with information they may need to respond to the incident.

I support today's proposed rules to enhance cyber practices by funds and advisers. And this is just one piece of the puzzle. This critical issue requires a comprehensive approach, and I look forward to future cyber-related Commission actions in other areas of our regulatory remit.[9]

Thank you to the Chair's office, the staff in the Division of Investment Management, the Office of the General Counsel, and the Division of Economic and Risk Analysis for their thoughtful work on today's proposal. I look forward to reviewing the comment letters and working with the staff as we move toward a final rule.

---

[1] Cybersecurity threat intelligence surveys consistently find the financial sector to be one of—if not the most—attacked industry. *See, e.g.*, IBM, X-Force Threat Intelligence Index 2021 (2021); PwC, Top Financial Services Issues of 2018 at 19 (2018) ("Criminals target financial firms because that's where the money is."); Carnegie Endowment for International Peace, Timeline of Cyber Incidents Involving Financial Institutions (last visited Feb. 9, 2022) (documenting approximately 200 cyber incidents targeting financial institutions since 2007).

[2] G20, Communique G20 Finance Ministers and Central Bank Governors Meeting Baden-Baden, Germany at 3 (Mar. 18, 2017)

[3] "Based on Form ADV filings up to October 31, 2021, there were 14,774 advisers with a total of $113 trillion in assets under management. Practically all (97%) of the advisers reported providing portfolio management services to their clients." Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies Release No. 33-11028 at 89 (proposed Feb. 9, 2022) [hereinafter "Release"]. "The funds that would be directly subject to the proposed rules include open-end funds, registered closed-end funds, business development companies, and unit investment trusts…In 2020, there were 15,750 registered funds, with over $25 trillion in net assets." *Id.* at 90.

[4] "Advisers and funds are exposed to, and rely on, a broad array of interconnected systems and networks, both directly and through service providers such as custodians, brokers, dealers, pricing services, and other technology vendors. Advisers also increasingly use digital engagement tools and other technology to engage with clients and develop and provide investment advice." *Id.* at 6.

[5] *See, e.g.,* FS-ISAC, Navigating Cyber 2021 (Mar. 2021) (detailing cyber threats that emerged in 2020 and predictions for 2021).

[6] "Meanwhile, the pandemic has exponentially accelerated digital transformation, making financial services both more interconnected and more competitive." *Id. See also* Release at n. 5.

[7] *See* Release at 15-44.

[8] *See* Release at 46.

[9] *See* Sec. & Exch. Comm'n, Agency Rule List – Fall 2021 (including a cybersecurity risk governance rulemaking proposal from the Division of Corporation Finance).