Sample SEC ADV-C

February 22, 2022

Form ADV-C

INVESTMENT ADVISER CYBERSECURITY INCIDENT REPORT PURSUANT TO RULE 204-6 [17 CFR 275.206(4)-6]

You must submit this Form ADV-C if you are registered with the Commission as an investment adviser within 48 hours after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident (collectively, "significant cybersecurity incident") has occurred or is occurring in accordance with rule 204-6 under the Investment Advisers Act of 1940.

Check the box that indicates what you would like to do (check all that apply):

- ☐ Submit an initial report for a significant cybersecurity incident.
- ☐ Submit an amended report for a significant cybersecurity incident.
- ☐ Submit a final amended report for a significant cybersecurity incident.

1. Investment Advisers Act SEC File Number: 801-
2. Your full legal name of investment adviser (if you are a sole proprietor, state last, first, middle name):
3. Name under which your primarily conduct your advisory business, if different from above:
4. Address of principal place of business (number, street, city, state, zip code):
5. Contact information for an individual with respect to the significant cybersecurity incident being reported: (Name, title, address if different from above, phone, email address)
6. Adviser reporting a:

- ☐ Significant cybersecurity incident
  a. If so, does the significant adviser cybersecurity incident involve and private funds?
     - ☐ Yes. Please list the fund ID number(s):
     - ☐ No

- ☐ Significant fund cybersecurity incident
  b. If so, list each investment company registered under the Investment Company Act of 1940 or company that has elected to be a business development company pursuant to section 54 of that Act involved and their SEC file number(s) (811 or 814 number) and the series ID number of the specific fund if more than one series under the SEC file number:

7. Approximate date(s) the significant cybersecurity incident occurred, if known:
8. Approximate date the significant cybersecurity incident was discovered:
9. Is the significant cybersecurity incident ongoing?
   - ☐ Yes
   - ☐ No. If not, approximate date the significant cybersecurity incident was resolved or any internal investigation pertaining to such incident was closed:
10. Has law enforcement or a government agency (other than the Commission) been notified about the significant cybersecurity incident?
    - ☐ Yes. If Yes, Which law enforcement or government agencies have been notified?
    - ☐ No

11. Describe the nature and scope of the significant cybersecurity incident, including any effect on the relevant entity's critical operations:
12. Describe the actions taken or planned to respond to and recover from the significant cybersecurity incident:
13. Was any data was stolen, altered, or accessed or used for any other unauthorized purpose?
    - Yes. If yes, describe the nature and scope of such information, including whether it was adviser information or fund information.
    - No
    - Unknown
14. Was any personal information lost, stolen, modified, deleted, destroyed, or accessed without authorization as a result of the significant cybersecurity incident?
    - Yes. If yes, describe the nature and scope of such information AND Has notification been provided to persons whose personal information was lost stolen damaged or accessed without authorization:
        - Yes
        - No. If no, are such notifications planned?
            - Yes
            - No
    - No
    - Unknown
15. Has disclosure about the significant cybersecurity incident been made to the adviser's clients and/or to investors in any investment company registered under the Investment 2223 Company Act of 1940 or company that has elected to be a business development company pursuant to section 54 of that Act, or private funds advised by the adviser involved?
    - Yes. When was such disclosure made:
    - No. Explain why no disclosure has been made:

16. Is the significant cybersecurity incident covered under a cybersecurity insurance policy maintained by you or any investment company registered under the Investment Company Act of 1940 or company that has elected to be a business development company pursuant to section 54 of that Act, or any private fund?
    - Yes. If Yes, Has the insurance company issuing the cybersecurity policy been contacted about the significant cybersecurity incident?
        - Yes
        - no
    - No
    - Unknown

Definitions

For the purposes of this Form:

Adviser information and adviser information systems have the same meanings as in rule 206(4)-9 under the Investment Advisers Act of 1940.

Fund information, fund information systems, and significant fund cybersecurity incident have the same meaning as in rule 38a-2 under the Investment Company Act of 1940.

Private fund has the same meaning as in section 202(a)(29) of the Investment Advisers Act of 1940. 2235

Personal information has the same meaning in rule 206(4)-9 under the Advisers Act of 1940 or rule 38a-2 under the Investment Company Act of 1940, as applicable.

Significant adviser cybersecurity incident has the meaning as in rule 204-6 under the Advisers Act of 1940.