File No. S7-04-22

SEC,

Please accept some questions on the Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies.

I generally support the proposal and believe transparency is key.

My questions relate to the legal requirements associated with a cyber event. There have been at least 2 major cyber attacks striking the fund and insurance industry in the past year; the MOVEit hack and the Infosys McCamish outage.

Open-end funds and UITs (including insurance products) are required to offer redeemable securities. This means that generally, purchases and redemptions must be processed at the NAV next computed and that redemption proceeds must be delivered within 7 days.

My question is, during a cyber event, can a fund or insurance company cease processing orders and withhold redemption proceeds if doing so is to protect investor information and assets? For example, in the Infosys McCamish outage, a few insurance companies offering variable products ceased processing transactions. This is because the service provider that processes transactions was infiltrated by a bad actor. To protect investor information and to preserve investor assets, these insurance companies (and retirement plan record keepers) ceased processing transactions, including redemptions. May funds and insurers cease processing transaction in order to protect investors without seeking emergency relief under section 22(e)? Is this situation comparable to the emergency weather event guidance published by the Commission in the rule 22e-2 adopting release? One concern is that 7 days is not sufficient time to request and receive section 22(e) relief. It usually takes days to figure out what is even going on in a cyber event. Also, the resolution time is also often a moving target. For example, originally Infosys McCamish stated that their outage would be resolved in 1 week, so section 22(e) was not necessary. Infosys McCamish kept extending that time such that the outage lasted for nearly 1 month.

So, how should a fund or insurance company respond to a cyber event in light of the various requirements of section 22 of the Investment Company Act of 1940? Are there best practices that funds and insurance companies should consider (in addition to providing investors notice as was proposed). Does the SEC expect a continuity of operations plan to include backup plans for all service provider functions that may be impacted by a cyber event? If section 22(e) emergency relief is required, can the SEC create a clear rubric explaining what information, undertakings and conditions the staff would require to help process any request for expedited relief. This way, funds can prepare for any such requirements even before a cyber event occurs.

Thank you,

Howie