CYBERSECURITY ADVISORY

To our valued SDDco client,

In recent months, the Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC) have both addressed the importance of Cybersecurity processes for the financial services industry by publicly releasing written guidance detailing current obligations and advisory procedures under existing law and regulations. Each of those releases were the subject of two SDDco Group Cybersecurity Advisory email installments in which we encouraged our clients to heed the advice of FINRA and the SEC to shore up their Cybersecurity procedures.

To further assist small firms in establishing an effective Cybersecurity program, FINRA offers a Checklist for a Small Firm's Cybersecurity Program ("Checklist") found here, which is derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and FINRA's Report on Cybersecurity Practices.

Found on FINRA's webpage, the Checklist is designed to help firm's create a

Cybersecurity program to (1) identify and assess cybersecurity threats and protect assets from cyber intrusion; (2) detect when systems and assets have been compromised; (3) plan for the response when a compromise occurs; and (4) implement a plan to recover lost, stolen or unavailable assets. FINRA suggests that "at a minimum, firms should know the assets that are vulnerable to a cyber-incident, and they should assign a risk level to these assets, [which will allow] executives to be informed on how best to allocate firm resources to protect the firm's and customers' information."

The Checklist is created once a firm answers a list of questions about their protected information, e.g. how it is transmitted and stored, its sensitivity, the devices used in storing said information, the impact of its loss on a business's operation, and the need to recover lost information. The responses to these questions leads the firm to create checklists for separate topics, such as inventory, information assets, encryption, controls and staff training, penetration testing, third party access, response plan, etc.

While it will help small firms understand more about the cyber threats most likely to affect their particular business, FINRA explains that "this checklist does not create a 'safe harbor' with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements." Instead, this Checklist should be used simply as a general overview to better understand the what, who, and how of Cybersecurity – i.e. what type of information needs to be protected, what devices are being used to protect it, who has access to said information, and how can we best protect said information. Firms still need to be prepared for more specific and detailed inquires during FINRA assessments.

In a recent routine cycle exam for an SDDco compliance client, FINRA asked: "**Please provide all of the firm's current procedures and policies**

established to protect client, trade, and confidential firm data, Password Management, Vendor Management, Patch Management, Security Training, Penetration Testing, Data Classification and Encryption, Change Management, and Incident Response, etc."

Certain cybersecurity procedures like, say, Penetration Testing, would not be sufficiently performed by a firm without a third-party vendor's service in place. As always, SDDco Group is here to help with your back office service needs, including the implementation of satisfactory Cybersecurity.

SDDco Group is developing a supplementary service that will provide our clients with state of the art Cybersecurity processes, including procedures like Penetration Testing. We expect to make these Cybersecurity services available to our SDDco clients in the coming months. Please anticipate its availability in the near term. Thank you for continuously trusting us with your regulatory support needs, and we look forward to addressing this Cybersecurity issue together.

Regards,
SDDco Group

RECAP:

FINRA's Checklist is designed to help firm's create a Cybersecurity program to:

- Identify and assess cybersecurity threats and protect assets from cyber intrusion
- Detect when systems and assets have been compromised
- Plan for the response when a compromise occurs
- Implement a plan to recover lost, stolen or unavailable assets

FINRA suggests that "at a minimum, firms should know the assets that are vulnerable to a cyber-incident, and they should assign a risk level to these assets, which will allow executives to be informed on how best to allocate firm resources to protect the firm's and customers' information."

FINRA explains that "this checklist does not create a 'safe harbor' with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements." Instead, this Checklist should be used simply as a general overview to better understand the what, who, and how of Cybersecurity. Firms still need to be prepared for more specific and detailed

inquires during FINRA assessments.

SPEAK TO A SDDco CONSULTANT

Are you interested in Broker-Dealer or Investment Advisor Registration, Compliance Consulting, Accounting, Tax or FinOp Services? You can reach us at info@sddco.com or 212-751-4422.

SDDco Is Support Made Simple

"When you hire SDDco, you benefit from the talent and expertise of the entire firm rather than that of an individual practitioner more limited in scope and resources."

SCOTT DANIELS
Co-Managing Partner