CONSTELLATION ADVISERS, LLC

REGULATORY NOTICE: 20-07

Hackers are using fake FINRA email addresses to phish registrants (actual phishing email below). For additional information, please see FINRA's Regulatory Notice on this subject here. As a result of this development, Constellation is providing this refresher on the U.S. Securities and Exchange Commission's ("SEC") cybersecurity focus areas.

Earlier this year, the SEC's Office of Compliance Inspections and Examinations ("OCIE") released its Cybersecurity and Resiliency Observations ("Cybersecurity Release"). View the full Cybersecurity Release here.

For your convenience, Constellation has summarized the Cybersecurity Release below, but please do not consider this refresher summary as all inclusive.

Cybersecurity and Resiliency Observations

In the Cybersecurity Release, OCIE identified the following key items.

Effective programs include governance and risk management with the following elements:

- Assessments to identify cybersecurity risks;
- Written policies and procedures to address those risks; and
- Implementation and enforcement of these policies and procedures.

New focus on mobile security. For mobile devices, firms should implement:

- Usage policies and procedures;
- Security measures to prevent copying, printing, or saving information to personal devices;
- Management applications or similar technology; and
- Employee training on proper usage.

In addition, OCIE emphasized the importance of effective controls, including:

- User access;
    - limit access to sensitive systems and data,
    - monitor system hardware and software changes,

- Access management;
    - periodic certifications,
    - require strong passwords,
    - multi-factor authentication,
    - revoke system access immediately for departed employees;
- Data loss prevention procedures;
    - vulnerability scanning,
    - perimeter and detective security,
    - patch management,
    - hardware and software inventory,
    - encryption and network segmentation,
    - insider threat monitoring, and
    - secure legacy systems and equipment.

Moreover, OCIE continues to highlight the features of effective incident response plans. Advisers' plans should include processes to:

- Comply with federal and state reporting requirements;
- File Suspicious Activity Reports ("SARs");
- Contact local authorities or the FBI and inform regulators;
- Share information with appropriate organizations; and
- Promptly notify clients and employees if their data has been compromised.

Lastly, OCIE encourages advisers to continuously:

- Monitor and test vendor relationships to confirm that their cybersecurity protocols meet appropriate standards; and
- Provide training to all employees on specific cybersecurity programs, especially phishing exercises.

Actual Phishing Email Purportedly From FINRA

From: *Josh Drobnyk <josh.drobnyk@broker-finra.org>*
Sent: *Monday, May 4, 2020*
To: *[Firm]*
Subject: *Action Required: FINRA Broker Notice for [Firm Name]*

Dear [Name],

I hope you are well and keeping safe.

I have been asked to send the attached document for [Firm Name] to you. They require immediate attention.

This is important and needs to be attended to before the end of this week.

Please let me know if you have any questions.

Kind regards,

Josh Drobnyk

Senior Vice President, Corporate Communications
FINRA Market Operations
[FINRA Address]

TAKE ACTION!

Clients Should:

- Be vigilant and cautious when receiving unexpected emails, even if they appear to be from a regulator.
- Examine their cybersecurity programs and advisory activities to confirm appropriate policies and procedures are in place to address the items identified above.
- Provide employees with a refresher on policies and procedures regarding cybersecurity.
- Test and verify that policies and procedures are functioning properly.
- Confirm the appropriate books and records are maintained to evidence compliance with regulatory requirements.
- Consider performing a mock exam to test your compliance program and to identify and correct potential deficiencies before undergoing an SEC exam.[1]

---

[1] In this Client Alert, Constellation is providing its observations, advice, and recommendations. Constellation did not and does not provide legal advice regarding its services nor did it or does it provide any assurance regarding the outcome of any future audit or regulatory examination or other regulatory action. It is further understood that recipients of this Client Alert have responsibility for, among other things, identifying and confirming compliance with laws and regulations applicable to their activities, and for establishing and maintaining effective internal controls to confirm such compliance.

Please contact a member of Constellation's Compliance team for assistance with any regulatory and compliance needs at compliance@constellationadvisers.com