Information Notice

Cybersecurity Alert: Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19)

March 26, 2020

Suggested Routing

- Compliance
- Legal
- Operations
- Registered Representatives
- Senior Management
- Systems

Key Topics

- Business Continuity Planning
- Cybersecurity

Summary

As work processes adjust in response to COVID-19, firms and their associated persons should take appropriate measures to address increased vulnerability to cybersecurity attacks and to protect customer and firm data on firm and home networks, as well as devices.

This alert provides firms and associated persons with measures they may use to help strengthen their cybersecurity controls in areas where risks may increase in the current environment. In particular, FINRA understands the resource challenges that small firms may face, but hopes that the information included below may help them address possible cybersecurity issues associated with remote work.

However, this alert does not provide an exhaustive list of steps that firms and associated persons should consider. Further, the alert is not intended to express any legal position, and does not create any new legal requirements or change any existing regulatory obligations.

FINRA is committed to providing guidance, updates and other information to help stakeholders stay informed about the latest developments on FINRA's COVID-19/Coronavirus Topic Page. New information will be posted on that webpage as it becomes available.

Questions concerning this *Notice* should be directed to:

- Dave Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or *david.kelley@finra.org*.

Background and Discussion

In recent weeks, FINRA has observed that firms have taken a number of steps to protect associated persons from the risks relating to COVID-19. In many cases, these measures include associated persons working in remote offices or using telework arrangements. The risk of cyber events may be increased due to use of remote offices or telework arrangements, heightened anxiety among

associated persons and confusion about the virus. While member firms are understandably focused on business resiliency and the health and safety of individuals, it is important that member firms remain vigilant in their surveillance against cyber threats and take steps to reduce the risk of cyber events. This alert outlines measures that firms and associated persons may take to address these risks.

Measures for Associated Persons

Office and Home Networks

- Use a secure network connection to access your firm's work environment (*e.g.*, through a company-provided Virtual Private Network (VPN) or through a secure firm or third-party website (which begin with "https").
- Secure Wi-Fi connections using a stringent security protocol (*e.g.*, WPA2).
- Check for and apply software updates and patches to routers on a timely basis.
- Change the default user names and passwords on home networking equipment, such as Wi-Fi routers.

Computers and Mobile Devices

- Check for and apply updates and patches to the operating system and any applications on a timely basis.
- Install and operate anti-virus (AV) and anti-malware software.[1]
- For any files on a personal device, check your firm's policy about file storage and back-up, especially if the files contain customer personally identifiable information (PII).
- Lock your screen if you work in a shared space and plan to be away from your computer.

Common Attacks

- Be sensitive to the growing variety of scams and attacks that fraudsters are using to exploit the current situation, such as:
  - phishing scams that reference COVID-19, the coronavirus or related matters;
  - fake, unsolicited calls from a "Helpdesk" requesting passwords or wanting to walk you through your home preparedness; and
  - malicious links in emails, online sites and unofficial download sides, especially those offering "free software."

Incident Response

- Understand your role in the firm's incident response plan and whom to contact in the event of a cybersecurity incident (*e.g.*, data breach, loss or exposure of customer PII, successful email attack, ransomware, lost or stolen mobile device).

Measures for Firms

Network Security Controls

Provide staff with a secure connection to the work environment or sensitive applications (*e.g.*, VPN, secure sessions[2] or remote desktop with multi-factor authentication).

- Evaluate privileges to access sensitive systems and data.

Training and Awareness

- Provide staff with training on:
  - how to connect securely to the office environment or office applications from a remote location; and
  - potential scams and other attacks described above.
- Alert the firm's IT support staff, or others involved in managing or supporting staff using the firm's systems, to be diligent in vetting incoming calls because fraudsters may use the increase in remote work to engage in social engineering schemes, such as making bogus calls requesting password resets or reporting lost phones or equipment. FINRA is aware of successful social engineering attacks where fraudsters contacted a Help Desk, for example under the guise of requesting a password reset, and subsequently used information about critical technical or business operations gained during this conversation to steal funds from the firm.

Contact Information

- Provide staff with important IT support staff contact information (*e.g.*, whom to call, how to contact them, when to contact them and how to handle emergency situations).

Additional Resources

- Defending Against COVID-19 Cyber Scams (US CERT)
- Scammers are Taking Advantage of Fears Surrounding the Coronavirus (Federal Trade Commission)
- Enterprise VPN Security (Department of Homeland Security)
- FINRA Cybersecurity Topic Page

Endnotes

1. This software is typically purchased on a subscription basis. FINRA has observed situations where individuals' subscriptions had lapsed, leaving the computer unprotected, even though the owner thought the software was still active.

2. An example of a "secure session" is connecting to your bank account through an encrypted website connection, *i.e.*, one with a URL address beginning "https:".