BLANKROME

Cybersecurity & Data Privacy

APRIL 22, 2020 • NO. 7

FINRA Releases Guidance to Aid Broker-Dealers in Combating Enhanced COVID-19 Cybersecurity Risks

Like other industries, broker-dealers have transitioned their workforces to remote working/teleworking arrangements as the coronavirus ("COVID-19") public health emergency has persisted. At the same time, broker-dealers also face a significantly heightened threat of cyber-attacks from malicious actors seeking to take advantage of the public's thirst for information about the virus, as well as other security vulnerabilities of remote working. Cognizant of these risks, the Financial Industry Regulatory Authority ("FINRA") issued two important pieces of guidance to ensure member firms remain vigilant in their surveillance against cyber threats and take steps to reduce the risk of cyber events. All broker-dealers should take time to review this guidance and, if feasible, implement the measures that have been suggested by FINRA to mitigate the increased cybersecurity risks that now exist due to COVID-19.

Regulatory Notice 20-08: Pandemic-Related Business Continuity Planning & Guidance

On March 9, 2020, FINRA issued Regulatory Notice 20-08, encouraging broker-dealers to review their business continuity plans ("BCP") and prepare their firms for the significantly enhanced cyber risks due to COVID-19 to minimize the risk of any disruptions in their operations. Notice 20-08 supplements prior FINRA guidance on pandemic preparedness issued in 2009 in connection with the outbreak of H1N1 (aka swine flu) but does not create new rules or obligations on member firms.

The guidance cautions firms that COVID-19 has led to an increased level of cyber risk, primarily due to increased work arrangements and the heightened fear and anxiety of employees relating to the public health emergency. It provides several action steps that firms can implement to mitigate those enhanced risks and threats, including the following:

- **Review Business Continuity Plans to Consider Pandemic Preparedness:** Firms should review their BCPs to consider pandemic preparedness, including whether the BCPs are sufficiently flexible to address a wide range of possible effects due to the COVID-19 pandemic. These effects may include staff absenteeism and personnel shortages, use of remote working or teleworking arrangements, travel/transportation limitations, and technology interruptions/slowdowns. In addition, firms must also ensure they have their appropriate emergency contacts in place to provide FINRA with a reliable means of contacting the firm in the event of an emergency.

- **Cybersecurity Measures:** As employees increasingly move to working remotely, firms are cautioned to consider the increased risk of cyber events as part of their pandemic-related preparedness. Firms must remain vigilant in their surveillance against cyber threats and take steps to reduce the risk of cyber events, including ensuring remote access systems have all available security updates, employing multi-factor authentication for all remote devices, and educating personnel of cyber risks and proper cyber practices and habits.

- **Assess Risk Mitigation Measures for Remote Offices or Telework Arrangements:** Where member firms have moved to remote offices or teleworking arrangements, firms must maintain a system that allows for the supervision of personnel who are working remotely during the pandemic. Firms should also test the broad use of remote offices or telework arrangements *prior* to activating their BCPs, including the ability to connect to critical firm systems, the adequacy of remote connectivity via residential Internet access networks, and any potential need to secure premium or dedicated service for connectivity.

- **Office Relocations:** If a firm relocates personnel to a temporary unregistered or non-branch location, the firm should provide written notification to its FINRA Risk Monitoring Analyst as soon as possible after establishing the new office or other work arrangement.

- **Adapting to Communications Challenges:** In the event a firm loses the ability to service its customers, it should promptly issue a notice on its website instructing customers on who to contact with respect to the execution of trades, account issues, and access to funds or securities.

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

On March 26, 2020, to further aid firms in mitigating the significantly enhanced cyber risks and threats as a result of COVID-19—especially as it relates to those associated with remote work—FINRA issued its Cybersecurity Alert offering measures firms can implement to help strengthen their cybersecurity controls in areas where risks may increase in the current environment. Like Regulatory Notice 20-08, however, this Cybersecurity Alert does not create any new legal requirements or change any existing obligations on member firms.

In particular, the Cybersecurity Alert provides the following recommended action steps for **firms:**

- provide personnel with a secure remote connection to the firm's networks and systems, such as through VPN or a secure remote desktop;

- evaluate employee privileges to access sensitive systems and data, and consider limiting privileges to only those necessary to allow employees to carry out their core job-related duties and responsibilities;

- provide training to staff on how to work remotely in a secure fashion, and on the heightened risk of potential cyber scams and attacks during the current health emergency;

- ensure IT support staff remains diligent to guard against the increased risk of social engineering schemes and other fraudulent behavior relating to remote work issues, such as bogus calls requesting password resets or reporting lost phones, as FINRA has noted an uptick in the frequency of successful social engineering attacks targeting company help desks with scams of this nature; and

- provide employees with contact information for key company personnel to alert in the event of an emergency situation so any incidents can be addressed and remediated as quickly as possible.

For **firm personnel,** the Cybersecurity Alert offers the following recommendations:

- use secured network connections to access firm work environments;

- ensure secure Wi-Fi connections;

- change all default user names and passwords on all personal devices;

- ensure to apply updates and patches to software, routers, operating systems, and applications in a timely manner;

- operate anti-virus and anti-malware software;

- adhere to firm policies relating to security measures for personal devices;

- be alert for growing number of scams and attacks that are being used to exploit the current health emergency, such as: (1) phishing scams that reference COVID-19; (2) fake, unsolicited calls from "helpdesks" requesting passwords; and (3) malicious links, especially those offering "free software"; and

- understand the employee's role in the firm's incident response plan and whom to contact in the event of a cyber-security incident.

Conclusion

Even before COVID-19 reached our nation's shores, broker-dealers and other financial entities were a top target of cyber criminals due to the vast amount of sensitive, high-value personal and financial information they possess. Moreover, the threats faced by financial institutions have grown significantly in recent years in both scale and sophistication as malicious actors enhance their capabilities and tactics.

Broker-dealers must be vigilant in guarding against the increased risk of cyber-attacks that now threaten firm operations as a result of COVID-19. Firms must take appropriate measures to effectively safeguard firm systems and networks, as well as consumer and firm data, from the enhanced threats that now exist as a result of the growing health crisis. In addition, firms must also address key cybersecurity issues associated with remote work, including properly educating employees on these risks and the threat of malicious actors seeking to take advantage of the outbreak, which will require extra care on the part of employees before supplying any sensitive information, clicking on any links, or transferring any funds or securities.

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity & Data Privacy team can assist with providing key counseling and guidance with respect to any issues or concerns relating to the implementation of FINRA's recommended cyber measures, as well as other policies, procedures, and protocols that broker-dealers should have in place to minimize the threat of cyber attacks to the greatest extent possible. And if your firm suffers a security incident during the ongoing public health crisis, Blank Rome's data breach incident response team is available 24/7 and can provide immediate assistance with rapid response and crisis management following any type of breach or security event.

For additional information, please contact:

Evan H. Lechtman, Philadelphia Office
Partner and Vice-Chair, Commercial Litigation
215.569.5367 | lechtman@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Cybersecurity & Data Privacy,
Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com