Report Underscores FINRA's Focus on Cybersecurity

January 18, 2023

On January 10, 2023, the Financial Industry Regulatory Authority ("FINRA") published its 2023 Report on FINRA's Examination and Risk Monitoring Program (the "Report"), which is intended to provide member firms with key considerations and observations to use in enhancing their compliance programs. The Report discusses 24 topics relevant to the securities industry, including cybersecurity, as cyber threats continue to evolve and present critical risks to many customers and firms.

The Report mentions several types of cybersecurity incidents that FINRA witnessed in 2022 that can expose member firms to financial losses, reputational risks and operational failures. These incidents include account takeovers, ransomware or network intrusions and associated exposure of customer information or fraudulent financial events. Relatedly, the Report reminds firms about cyber-related regulatory obligations, including Rule 30 of the U.S. Securities and Exchange Commission's ("SEC") Regulation S-P and Regulation S-ID (Identity Theft Red Flags) and Exchange Act Rules 17a-3 and 17a-4 (Books and Records) as well as FINRA Rules 4370 (Business Continuity Plans and Emergency Contact Information), 3110 (Supervision) and 3120 (Supervisory Control System).

This post discusses FINRA's continued focus on cybersecurity as well as key insights and effective practices from the Report for firms to consider for their cybersecurity programs.

FINRA's Continued Focus on Cybersecurity. The Report illustrates FINRA's significant focus on cybersecurity, including its creation of the Cyber and Analytics Unit in August 2022. The Report incorporates many of the lessons learned from FINRA's public guidance, reports, enforcement actions and regulatory notices. FINRA regularly updates its Cybersecurity Topic Page and has published numerous resources, including its 2015 Report on Cybersecurity, 2018 Report on Selected Cybersecurity Practices, Firm Checklist for Compromised Accounts, Cross Market Options Supervision: Potential Intrusion Report Card, Small Firm Cybersecurity Checklist and Core Cybersecurity Threats and Effective Controls for Small Firms. FINRA has also issued a series of regulatory notices that discuss risks associated

with ransomware, digital signature falsification, software vulnerabilities, phishing, third-party vendors, compromised customer accounts, new account schemes and imposter websites.

Considerations and Effective Practices Related to Cybersecurity. The Report provides firms with insights as to what FINRA views as effective practices that comply with cybersecurity regulatory obligations as well as methods to address evolving cybersecurity threats, including:

- **Risk Assessments:** To develop and maintain robust cybersecurity practices, firms should perform risk assessments periodically to assess their risk profiles, making sure to account for any changes to the nature and scope of firm activities, current cybersecurity practices, active and potential threats and industry best practices. Risk assessments are important for identifying and preventing potential cybersecurity intrusions like ransomware, phishing and more. Firms can help reduce cybersecurity risks by training staff in organizational security practices, such as digital hygiene and phishing awareness.

- **Written Supervisory Procedures and Incident Response Planning:** The risk assessments described above can help inform written supervisory procedures ("WSPs"). The FINRA report lays out several practices that firms can include in their WSPs, such as protected storage so that firms regularly back up critical data. In addition, firms should consider developing an incident response plan ("IRP") that explains responsibilities and actions for appropriate firm staff to take in the event of a cybersecurity event, including how the firm will restore its systems and how it will recover any impacted data.

- **Authorized System Access:** To help ensure that only authorized employees, customers and contractors can access a firm's systems, firms should consider implementing multifactor authentication for employees, contractors and customers.

- **Monitoring New Accounts:** New customer accounts can also present external threats, so businesses should consider validating the identity of customers opening new accounts and monitoring suspicious activity, such as the opening of multiple new accounts from the same IP address. Firms can use third parties to help verify identities and obtain risk assessments for new accounts to determine if additional safeguards should be implemented.

- **Data Loss Prevention:** Failure to monitor activity within a firm's system, such as unauthorized copying, downloading or deletion of data, can lead to increased cybersecurity risks. Similarly, lack of controls on outbound communications can place sensitive customer and firm information at risk. Firms should consider

implementing technology that can scan outbound communications to identify and restrict sensitive or confidential customer or firm data as well as controls on internal network activity. Additionally, sufficient data-log management practices can help firms determine the onset and scope of a cyber-attack that results in data loss, while adding secure settings to firm software can reduce system vulnerabilities.

- **Third-Party Vendor and Supply Chain Risks:** In establishing relationships with third-party vendors, firms should be aware of the risks that a cybersecurity incident at the third party can have on them. Firms are encouraged to assess these risks during the onboarding process and maintain records of the services, systems and software components that the third party provides and how any of those items interact with the firm's infrastructure.

- **Cloud Computing:** Cloud computing services are increasingly popular because they can provide increased data storage, processing capacity and networking opportunities. At the same time, cloud computing can present increased risk if not adopted thoughtfully. Firms shifting to cloud services should consider how they will divide cybersecurity risk management tasks with their cloud provider as well as how potential cloud service providers account for cybersecurity threat detection, incident response and patching.

- **Imposter Domains:** Threat actors may attempt to impersonate firms on the internet, potentially causing monetary and reputational damage. Firms are encouraged to monitor for imposter websites and create plans to address such websites upon detection.

- **Reporting Suspicious Activity:** Businesses should review regulatory obligations around filing suspicious activity reports ("SARs") and develop procedures to report cybersecurity incidents internally and externally according to those obligations. FINRA also noted that firms should be aware of any applicable guidance that the Financial Crimes Enforcement Network ("FinCEN") issues when evaluating whether to file a SAR in light of a cyber event.

- **Branch Controls:** The Report also provides branch-specific cybersecurity insights, including that firms should consider: (1) how to identify and confront cybersecurity risks that stem from branch-hosted email and other software applications; (2) developing a technology asset inventory capable of monitoring authorized access to firm systems and data; (3) strategies for maintaining compliance at the branch level with a firm's cybersecurity standards established in its WSP; (4) whether to use branch-managed servers for functions such as email or other applications (e.g., customer relationship management, reporting) and, if branch-managed servers are allowed, how to implement appropriate security controls to oversee such functions;

and (5) how to ensure that branch-office personnel know how to effectively respond to cybersecurity events that occur in the branch office, including any reporting requirements to the home office.

* * *

The authors would like to thank Debevoise law clerk Ned Terrace for his contributions to this post.

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Charu A. Chandrasekhar
cachandrasekhar@debevoise.com

SAN FRANCISCO

Michael R. Roberts
mrroberts@debevoise.com

Kristin A. Snyder
kasnyder@debevoise.com