Updates
August 14, 2020

SEC and FINRA Provide Guidance Regarding Cybersecurity, Artificial Intelligence, and Digital Assets

The U.S. Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) made several regulatory announcements this summer relating to cybersecurity, artificial intelligence (AI), and digital assets. These announcements are detailed below and include a FINRA summary report on the uses of AI in the securities industry, a FINRA regulatory notice regarding its members' activities relating to digital assets, and a risk alert from the SEC's Office of Compliance Inspections and Examinations (OCIE) on increased cybersecurity threats.

FINRA Publishes Report Detailing AI Usage in Securities Industry

On June 10, 2020, FINRA issued a summary report regarding existing and emerging uses of AI by securities industry participants. For a more detailed discussion of FINRA's summary report, please see our previous update .

FINRA Renews Request to Member Firms to Provide Notification of Digital Asset Activities

On July 9, 2020, FINRA reissued a request that member firms continue to proactively engage with their FINRA risk monitoring analyst regarding any type of digital asset activity, current or planned, similar to requests made in 2018 and again in 2019. The 2019 regulatory notice was set to expire on July 31, 2020, and through its 2020 regulatory notice (FINRA Regulatory Notice 20-23), FINRA extended the request through July 31, 2021.

Like its previous regulatory notices, FINRA requests that its members promptly notify their risk monitor analysts of any current or potential activity relating to digital assets. For purposes of its 2020 regulatory notice, FINRA defined "digital assets" as "cryptocurrencies and other virtual coins and tokens . . . and any other asset that consists of, or is represented by, records in a blockchain or distributed ledger (including any securities, commodities, software, contracts, accounts, rights, intangible property, personal property, real estate or other assets that are 'tokenized,' 'virtualized' or otherwise represented by records in a blockchain or distributed ledger)." With its broad definition of "digital assets," FINRA's request for proactive notification includes any digital asset activities, regardless of whether the relevant digital assets are "securities" under the federal securities laws.

In addition to its request, FINRA provided a list of activities that would elicit notification, including, but not limited to, the following:

- Purchases, sales, or executions of transactions in digital assets
- Purchases, sales, or executions of transactions in a pooled fund investing in digital assets
- Creation, management, or provision of advisory services for a pooled fund related to digital assets
- Purchases, sales, or executions of transactions in derivatives (e.g., futures, options) tied to digital assets
- Participation in an initial or secondary offering of digital assets (e.g., ICO, pre-ICO)
- Creation or management of a platform for the secondary trading of digital assets

- Custody or similar arrangement of digital assets
- Acceptance of cryptocurrencies (e.g., bitcoin) from customers
- Mining of cryptocurrencies
- Recommending, soliciting, or accepting orders in cryptocurrencies and other virtual coins and tokens
- Displaying indications of interest or quotations in cryptocurrencies and other virtual coins and tokens
- Providing or facilitating clearance and settlement services for cryptocurrencies and other virtual coins and tokens
- Recording cryptocurrencies and other virtual coins and tokens using distributed ledger technology or any other use of blockchain technology

With its request renewal FINRA is continuing to track and monitor members' digital assets use and exposure. It is constantly assessing the roles and behaviors of its members relating to digital assets in addition to the attendant risks. From a regulatory risk mitigation perspective, it is generally important for members operating in the digital asset space to foster open dialogue with FINRA and the SEC. Further, depending on the activities, pursuant to FINRA rules, a continuing membership application may be required, or at a minimum, it may be prudent to submit a materiality consultation.

OCIE Issues Risk Alert on Cybersecurity and Ransomware

On July 10, 2020, OCIE issued a Cybersecurity risk alert on the risks of ransomware. Ransomware is a type of malware designed to provide an unauthorized actor access to an institution's systems and to deny the institution's use of those systems until a ransom is paid. OCIE explained in its risk alert that it is aware of recent reports that one or more bad actors have orchestrated phishing and other campaigns designed to penetrate and deploy ransomware attacks on SEC registrants, including broker-dealers, investment advisers, and investment companies.

In light of the uptick in recent ransomware attacks and threats, OCIE provided guidance to registrants to enhance their ransomware prevention. In doing so, OCIE noted that there is no "one-size-fits-all" and every registrant should consider its own circumstances and risks when devising a cybersecurity program that includes ransomware attack prevention as detailed below:

- **Incident response and resiliency policies, procedures, and plans:** Design and implement response and resiliency policies, procedures, and plans that address what the response should be and how it should be orchestrated in the event of a ransomware attack. Such policies and plans include instructions on whom to notify in the event of a ransomware attack (e.g., internally within the organization as well as law enforcement) and how to manage any applicable federal or state regulatory reporting requirements.
- **Operational resiliency:** Determine which critical applications can be maintained or restored during a disruption and ensure a geographic separation of backup data and writing backup data to an immutable storage system to ensure access during a disruption.
- **Awareness and training programs:** Train employees on cybersecurity and resiliency, including on how to identify phishing emails.
- **Vulnerability scanning and patch management:** Ensure that any programs designed to scan and catch ransomware, viruses, or malware are up to date and that they are designed for the current technology environment.
- **Access management:** Manage access to systems by limiting access as necessary, requiring strong passwords, considering multifactor authentication, and revoking access immediately once an individual is no longer employed by the registrant.
- **Perimeter security:** Implement perimeter security controls, such as firewalls, intrusion detection systems, email security capabilities, and web proxy systems. These can help a registrant control and monitor access

to the internet in order to address potential security vulnerabilities of internet connections.
- **Familiarization with existing guidance:** Review the existing cybersecurity guidance noted by OCIE throughout the risk alert from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation, and OCIE

As noted above and in a discussion of OCIE's January 2020 cybersecurity guidance, OCIE and the SEC have long been focused on cybersecurity issues and previously indicated a heightened focus for 2020. This risk alert is the latest in discussions and guidance on the relevant threats to SEC registrants as well as potential steps that registrants should consider to protect themselves and their customers' information.

Please contact experienced securities regulatory counsel with any questions about these developments and their applications to an individual or business.

Explore more in

Investment Management Blockchain & Digital Assets Fintech & Payments Artificial Intelligence & Machine Learning

Related insights

Update

Why the FCC’s Net Neutrality Rules Were Struck Down

Update

Proposed DOJ FARA Rules Would Increase Uncertainty for Global Companies Amid Heightened Enforcement