SEC Cybersecurity Fines and the Importance of Multi-Factor Authentication

September 28, 2021

In case you hadn't heard, the Securities and Exchange Commission recently fined eight financial firms a total of $750,000 over email hacks that exposed client data. The SEC found that the firms had inadequate cybersecurity protections, which led to the exposure of personally identifiable information of thousands of customers and clients after hackers took over employee email accounts.

Despite what their own cybersecurity policies mandated, these firms did not have multifactor authentication (MFA) in place. The SEC found these firms in violation of the "Safeguards Rule," more formally known as Rule 30(a) of Regulation S-P, which is designed to protect confidential customer information.

Ouch. As we've said before, it is not enough to have a cybersecurity policy, the policy must be implemented, actively monitored, and enforced in order for it to be defendable (and for the firm to stay protected).

Ironically, we chose to address the importance of MFA in our August Tech Trends blog Ransomware Attacks Are Closer Than You Think. Given recent headlines, we thought it was important to reiterate the best practices for staying secure:

- **Implement adaptive MFA and end device management** – used in combination, these tools can prevent most cybersecurity attacks.
- **Don't click on any links or attachments inside phishing emails**. Doing so instantly compromises the email account and puts the firm's IT network into the hands of a criminal or criminal network.
- **Never upload or offer your credentials unless you are expecting to access a known system**. When in doubt, don't enter anything in and call your IT support team.
- **Have your IT support team implement a cybersecurity training and testing** program for your entire organization on data protection and cybersecurity protocols.
- **Pay attention to the senders of inbound emails.** "Spoofed" email addresses look similar enough to a legitimate address and can trick the unsuspecting receiver into giving away access or information to a cyberthief.

We can't overstate the importance of keeping your network secure. A hacked system –

whether through compromised email or other means – can have severe and even devastating consequences, not only for the firms that are attacked, but for the individuals and families whose personal and financial information ends up in the hands of bad actors.