SEC Enforcement Case Summary
Failure to Protect Client Funds Against Cyber Intrusions

On August 20, 2024, the SEC announced a settled action against transfer agent Equiniti Trust Company LLC (formerly American Stock Transfer & Trust Company) for failing to assure that client securities and funds were protected against theft or misuse. Those failures led to the loss of more than $6.6 million of client funds as a result of two separate cyber intrusions in 2022 and 2023.

In September 2022, an unknown threat actor hijacked a pre-existing email chain between what was then American Stock Transfer and a U.S.-based public-issuer client. The threat actor, pretending to be an employee at the issuer, instructed American Stock Transfer to issue millions of new shares of the issuer, liquidate those shares, and send the proceeds to an overseas bank. The SEC's order notes that the threat actor concealed its identity by using an email domain that was almost identical to the real issuer's domain except for one letter, by imitating the verbal patterns and practices of firm contacts, and by sending fraudulent instructions as a continuation of an existing email chain rather than a standalone request. The relevant American Stock Transfer employee replied to the email to verify the instruction, but the reply went to the altered email address rather than the issuer. As a result, the firm followed the fraudulent instructions and transferred approximately $4.78 million to bank accounts located in Hong Kong.

In an unrelated incident in April 2023, an unknown threat actor used stolen social security numbers of certain American Stock Transfer accountholders to create fake accounts that were automatically linked by American Stock Transfer to real client accounts based solely on the matching social security numbers, even though the names and other personal information associated with the fraudulent accounts did not match those of the legitimate accounts. This allowed the threat actor to liquidate securities held in the legitimate accounts and transfer a total of approximately $1.9 million in proceeds to external bank accounts.

The SEC noted in its case that in advance of these incidents, the firm sent communications to relevant employees involved in processing client payments alerting them to increasing industry-wide incidents of fraud and warning them to be on alert for fraudulent wire transfer requests. The email provided further guidance on steps to take to identify fraudulent requests and verify client instructions. The firm is faulted for not implementing the safeguards or procedures outlined in the email, such as confirming that employees read the communication, providing additional training, or monitoring to ensure that employees performed the risk mitigation steps that were outlined.

This action highlights the increasing sophistication of hackers and threat actors in devising schemes to steal money and emphasizes the need for increased vigilance to train employees and monitor for compliance with established controls to mitigate risks. Although American Stock Transfer was ultimately able to recover approximately $2.6 million of the losses resulting from these incidents and fully reimbursed the clients for their losses, Equiniti nevertheless agreed to pay a civil penalty of $850,000 to settle the case. The SEC acknowledged the firm's cooperation and additional remedial steps that it took voluntarily, including hiring a Chief Control Officer responsible for overseeing cyber security and engaging a third-party cyber security firm to conduct a forensic review of Respondent's systems.

See Summary - https://www.sec.gov/newsroom/press-releases/2024-101