SEC CYBER UPDATE

NEW RULES ON CYBERSECURITY DISCLOSURES, ENFORCEMENT, AND OTHER CURRENT PRIORITIES

UT Law CLE Essential Cybersecurity Law

October 26, 2023

1

SEC CYBER AUTHORITY

- Enforcement Division
  - Public Company Disclosures
  - Regulated Entities Compliance
  - Cyber and Crypto Unit
- Exams Division

2

PUBLIC COMPANY ENFORCEMENT

- In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc. (2018)
  - First SEC enforcement action related to cyber disclosures
  - Allegedly knew of a data breach by late 2014
  - Failed to disclose the data breach in public filings for nearly two years
  - Submitted quarterly and annual statements from 2014 to 2016 that were materially misleading about the breach
  - $35 million civil penalty
  - "We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case," said Steven Peikin, Co-Director of the SEC Enforcement Division.

PUBLIC COMPANY ENFORCEMENT

- Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements
  - Enforcement Division investigated whether certain public issuers that were victims of cyber-related frauds may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls
    - Emails from fake executives
    - Emails from fake vendors
  - "[I]nternal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds."

PUBLIC COMPANY ENFORCEMENT

- In the Matter of First American Financial Corporation (2021)
  - Notified of a breach by a cybersecurity blogger
  - Issued a Form 8-K saying the company had just learned of the vulnerability and took immediate action
  - But the company's InfoSec team allegedly had known about the vulnerability for months and had not fully remediated it
  - Executives drafting public statements were not aware
  - SEC charged the company with deficient disclosure controls related to cybersecurity
  - $487,616 civil penalty

PUBLIC COMPANY ENFORCEMENT

- In the Matter of Pearson plc (2021)
  - Pearson allegedly suffered a data breach in 2018, but didn't immediately disclose it
  - In filings with the Commission, Pearson referred to a data privacy incident merely as a hypothetical risk, even though a material breach had already occurred
  - When the breach became public, allegedly made misleading statements and omitted material information about the scope of the breach and the company's cyber protections
  - The SEC charged the company for the misleading statements and for deficient disclosure controls and procedures
  - $1 million civil penalty

Title search: SEC Cyber Update: New Rules on Cybersecurity Disclosures, Enforcement, and Other Current Priorities

First appeared as part of the conference materials for the
2023 Essential Cybersecurity Law session
"SEC Cyber Update: New Rules on Cybersecurity Disclosures, Enforcement, and Other Current Priorities"