Published on *The National Law Review* https://natlawreview.com

Facebook SEC Enforcement Action Has Important Implications for Cybersecurity Whistleblowing

Article By:

Dallas Hammer

Jason Zuckerman

On July 24th, the U.S Securities and Exchange Commission announced that Facebook, Inc. has agreed to pay $100 million to resolve charges that Facebook made misleading disclosures regarding the risk of misuse of user data. This development shows the significant consequences of failing to accurately disclose cybersecurity risks and underscores the incentives that encourage cybersecurity whistleblowers to come forward. Just as courageous whistleblowers such as Sherri Watkins and Cynthia Cooper played a vital role in exposing the accounting fraud that resulted in a near market meltdown about two decades ago, whistleblowers at technology companies are positioned to serve a prominent role in addressing emerging challenges in the cybersecurity field.

$100M Facebook Enforcement Action

According to the SEC's complaint, in 2014 and 2015, the now-defunct advertising and data analytics company, Cambridge Analytica used a third party to collect and transfer data from Facebook to profile about 30 million Americans. In addition, the third party transferred to Cambridge Analytica the underlying Facebook user data, including names, genders, locations, birthdays, and "page likes," in violation of Facebook's policies. Ultimately, Cambridge Analytica used this information in connection with its political advertising activities.

In 2015, Facebook discovered the misuse of user data but did not correct its existing risk disclosure for more than two years, according to the SEC's complaint. Instead, Facebook continued to make vague, hypothetical disclosures to investors warning that its "users' data may be improperly accessed, used or disclosed." According to the complaint, Facebook reinforced this false impression by telling news media investigating Cambridge Analytica's use of Facebook user data that it had not discovered evidence of wrongdoing. In 2018, Facebook finally disclosed the incident, which precipitated a decline in its stock price. The SEC concluded that Facebook filed materially misleading periodic reports and knew, or should have known, that its risk factor disclosures in its annual reports were materially misleading.

The SEC also alleged that during this two-year period, Facebook failed to maintain disclosure controls and procedures designed to analyze or assess incidents involving misuse of user data for

potential disclosure in the company's periodic filings. Facebook resolved the claims without admitting or denying them.

Implications of Facebook Enforcement Action for Public Companies

This enforcement action is consistent with two prior SEC enforcement actions in which the SEC sent a strong message that it expects public companies to provide accurate disclosures about information security risks and mitigate those risks:

- In 2015, the SEC took one of its first cybersecurity-related enforcement actions in the matter of R.T. Jones Capital Equities Management, Inc. In that case, the Commission fined an investment adviser for failing to ensure that its third-party service providers had adequate cybersecurity measures to protect customer data.
- In April 2018, the SEC charged the entity formerly known as Yahoo!, Inc., with failing to disclose a mega-breach to shareholders in a timely manner. The entity, now called Altaba, agreed to pay $35 million to resolve the charges.

The Facebook enforcement action demonstrates how the SEC's bread-and-butter enforcement authority can be a potent tool for the SEC to regulate cybersecurity issues. Notably, the SEC applied statutes enacted in 1933 and 1934 – long before computers were around, much less social media – to effectively redress a high-profile scandal exemplifying the emerging and varied challenges posed by the digital age. The $100M penalty should cause public companies to assess the adequacy of their information security controls and the accuracy of their cybersecurity risk disclosures.

Implications of Facebook Enforcement Action for Cybersecurity Whistleblowers

The enforcement action against Facebook also suggests that whistleblowers will continue to play a vital role in exposing cybersecurity failures and risks. Specifically, it indicates that cybersecurity whistleblowers are afforded protection against retaliation under the Sarbanes-Oxley Act and are potentially eligible for a whistleblower reward under the SEC Whistleblower Program created by the Dodd-Frank Act.

First, the action confirms our view that information security professionals at public companies are protected against retaliation for disclosing deficient cybersecurity in that cybersecurity vulnerabilities or failures implicate potential violations of federal securities laws and therefore fall within the ambit of the Sarbanes-Oxley whistleblower protection law. The SEC's theory in the Facebook action applies a variation of the half-truth doctrine that could render omissions of known cybersecurity deficiencies to be material misrepresentations. In addition, the complaint also demonstrates that when a breach or misconduct results from a public company's failure to adopt and maintain adequate internal controls, a company can be liable for violating the internal controls provisions of the Sarbanes-Oxley Act.

Second, this enforcement action shows that the Commission's Whistleblower Rewards Program is a viable option for cybersecurity whistleblowers to come forward anonymously and potentially qualify for an SEC whistleblower award. Typical cybersecurity-related enforcement actions may not exceed the $1M threshold necessary to qualify for an SEC whistleblower award, but when a public company's failure to take reasonable cybersecurity measures or to disclose known cybersecurity issues results in harm to the company's customers and shareholders, whistleblowers disclosing these violations could qualify for an SEC whistleblower award.

National Law Review, Volumess IX, Number 209