SECURITIES CLIENT ALERT

When Data Misuse Has Occurred, the Risk is No Longer "Hypothetical"

By: Jeffrey T. Haughey and Andrew R. Polly

August 9, 2019

On July 24, 2019, the U.S. Securities and Exchange Commission (SEC) announced charges against Facebook for making misleading disclosures regarding the risk of misuse of Facebook user data. According to the SEC, Facebook framed the improper use of user data as a *hypothetical* investment risk in its Form 10-Ks and Form 10-Qs for more than two years, despite Facebook's knowledge that the data had already been misused by a third-party developer. The result? The SEC viewed the mischaracterization in Facebook's public filings as a misleading disclosure, and forced Facebook to a pay a $100 million settlement.

In its complaint, the SEC emphasized its expectation that public companies identify and consider the material risks to their businesses and implement procedures designed to provide accurate disclosures. While Facebook resolved the claims without admitting or denying the allegations, the company was permanently enjoined from violating Sections 17(a)(2) and (3) of the Securities Act of 1933, and Section 13(a) of the Securities Exchange Act of 1934 (the "Act"), as well as, several rules under the Act related to disclosure.

The SEC's enforcement proceeding against Facebook is a reminder of the potential significant consequences for having inadequate disclosure controls and procedures and inaccurate cybersecurity risk disclosures.

Disclosure Controls - Who Needs to Know What?

It is no surprise that Facebook's financial success is largely dependent on the size of its user base. By failing to report incidents that could create user distrust, Facebook created a false impression of security for its investors.

© 2019

The SEC criticized Facebook for failing to maintain appropriate controls and procedures for disclosure. These controls are designed to analyze incidents and generate reports for departments responsible for drafting a company's public filings. While employees in Facebook's legal, policy, and communications group were aware of the improper data transfer, the incident was not discussed in quarterly meetings regarding the company's earnings announcements. In addition to its internal shortcomings, Facebook did not disclose the data transfer incident to its independent auditors or outside counsel who could have further assessed the company's disclosure obligations.

Next Steps - Update Your Disclosures Controls and Procedures

Outlining a mechanism for reporting relevant information to employees responsible for submitting accurate filings will ensure your company does not materially mislead investors or provide inaccurate reports to the SEC. Using Facebook as an example, it may be time to update your disclosure controls and procedures.

If you have questions about information security, cybersecurity risks, or related disclosures controls and procedures, feel free to contact any attorney in our Corporate & Securities Law Practice.

Jeffrey T. Haughey
(918) 595-4837
jhaughey@gablelaw.com

Andrew R. Polly
(918) 595-4850
apolly@gablelaw.com

The authors would also like to thank summer associate Emma Kincade for her invaluable research and drafting of this client alert.

GableGotwals
1100 ONEOK Plaza
100 West Fifth Street
Tulsa, OK 74103-4217
www.gablelaw.com

This article is provided for educational and informational purposes only and does not contain legal advice or create an attorney-client relationship. The information provided should not be taken as an indication of future legal results; any information provided should not be acted upon without consulting legal counsel.

© 2019