MASSACHUSETTS LAWYERS WEEKLY

Lesson from Yahoo! case: Heed disclosure requirements!

By: Joseph J. Floyd - August 23, 2018

Proper reporting for public registrants involves much more than producing financial statements in accordance with generally accepted accounting principles. In fact, the disclosures made in public filings may be as or more important and meaningful to financial statement users than what is reported on the financial statements alone.

In Item 303(a) of Regulation S-K, the U.S. Securities and Exchange Commission requires that a public registrant discuss its financial condition, changes in financial condition, and results of operations in the company's management discussion and analysis section of its public filings.

The requirements include identifying "any known trends or any known demands, commitments, events, or uncertainties that will result in or that are reasonably likely to result in the registrant's liquidity increasing or decreasing in any material way."

Another major requirement is to report "any known trends or uncertainties that have had or that the registrant reasonably expects will have a material favorable or unfavorable impact on net sales or revenues or income from continuing operations."

Complying with Item 303(a) means companies must open the door to senior management discussions and share a significant amount of information with investors. Not surprisingly, for many management teams, sharing positive news is easy, whereas openly sharing information regarding problems is not.

A recent SEC Accounting and Auditing Enforcement Release regarding the settlement of an action against Altaba Inc. (the "company") provides a very useful example of the failure to comply with disclosure requirements for an unfavorable event that involved a material data breach of personal customer information. The company is better known by its former name, Yahoo! Inc.

Of great concern, the SEC indicates that many people in the company, including senior executives, had complete transparency regarding the extent of the data breach and its risks to the company, yet the information was withheld from the shareholders for almost two years.

Below is a summary of the key facts in the case, including what the company knew compared to what it contemporaneously disclosed, as well as observations that will help audit committees and those that advise public registrants to avoid similar lapses in judgment.

Background

Per the AAER, the company in late 2014 learned of a "massive breach of its user database that resulted in the theft, unauthorized access, and acquisition of hundreds of millions of its users' data, including usernames, birthdates, and telephone numbers" by hackers associated with the Russian Federation.

Almost immediately, the company's senior management and legal teams received various internal reports from the company's chief information security officer describing the severity of the problem. Of note, the SEC conveys that the company's senior management and legal teams did not report the situation to the company's auditors or outside counsel.

The situation worsened in 2015 and 2016 as the company's information security team determined that the same hackers were continuously targeting the user database.

The information security team also received reports raising the possibility of a high volume of compromised user credentials for sale on the dark web.

In fact, according to the SEC, in June 2016, the company's new chief information security officer (hired in October 2015) concluded that Yahoo's entire user database, including the personal data of its users, had likely been stolen by "nation-state actors" through several hacker intrusions (including the 2014 breach), and ultimately could be exposed on the dark web in the immediate future.

The release states that the new chief information security officer communicated those conclusions to at least one member of the company's senior management while the company was negotiating the sale of its operating business to a major telecommunications business.

Yet the company still made no public disclosure of the problem and, to the contrary, affirmatively represented that it was unaware of any security breaches in its stock purchase agreement with the telecommunications business, a document subsequently filed as an exhibit to a Form 8-K on July 25, 2016, and therefore a public record.

The SEC alleged that the company failed to disclose the data breach in any public filings until the third quarter of 2016, making its 2014 and 2015 Form 10-Ks and Form 10-Qs for the first three quarters of 2015 and the first two quarters of 2016 deficient and misleading.

Remarkably, the company's disclosures in its annual and quarterly reports from 2014 through 2016 reported that it had faced only the "risk of potential future data breaches" that might expose the company to adverse consequences and did not disclose such a breach had in fact already occurred. The disclosures in the public filings during the time periods included the following statements:

"[p]roducts and services involve the storage and transmission of Yahoo's users' and customers' personal and proprietary information in our facilities and on our equipment, networks, and corporate systems."

"If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure."

"[s]ecurity breaches expose us to a risk of loss of this information, litigation, remediation costs, increased costs for security measures, loss of revenue, damage to our reputation, and potential liability."

Yet, the breach had occurred and describing the risks with an "if" qualifier did not match reality, as the consequences were not theoretical but rather were imminent.

Market evidence for the materiality of the breach occurred in September 2016, when the company disclosed the 2014 data breach and its market capitalization dropped approximately $1.3 billion due to a 3 percent decrease in its stock price. Further evidence of the materiality of the breach is found in the renegotiation of its stock purchase agreement described above and the reduction to the price for the company's operating business of $350 million, representing a 7.25 percent reduction.

Not surprisingly, when the company finally disclosed the problem in its Form 10-Q for the third quarter of 2016, it stated that the company expected to incur expenses — including investigation, remediation and legal costs — related to the 2014 breach.

Also not surprising, in its 2016 Form 10-K, the company disclosed that its principal executive officer and principal financial officer had concluded that, "due exclusively to deficiencies in the Company's existing security incident response protocols related to the 2014 Security Incident, the Company's disclosure controls and procedures for each of the annual and quarterly periods ended December 31, 2014 through September 30, 2016 were not effective at the end of each such period."

The settlement with the SEC included a cease and desist order, a $35 million civil penalty, and a cooperation agreement with the company related to any and all other proceedings arising out of the situation.

Needless to say, the cooperation agreement indicates that the SEC may be bringing other actions soon. Based on a review of the facts discussed above in the SEC's AAER, it is understandable why further actions may be forthcoming.

Observations, recommendations

Having reviewed the company's failures to comply with proper disclosures and to have controls in place for all information, good and bad, to be vetted, raises the obvious question of what can be done to avoid similar situations.

Situations in which senior management suppresses information may make traditional disclosure committees and processes useless. However, old-fashioned employee training and whistleblower hotlines can be an audit committee's strongest ally to ensure facts are vetted properly, assessed and disclosed. The AAER makes no mention of whether the company had such training or hotlines.

In addition, noting the risk disclosure in place for the company, targeted questions by the audit committee for updates may have brought the problem to a board-level discussion.

Such questions of management should include, but not be limited to, previously disclosed risk factors and should encompass industry-wide risks and concerns. For the company, the entire industry has been under pressure for data breaches and hacking.

Finally, and possibly among the most notable and troubling observations from the AAER is the lack of any discussion with outside counsel regarding the data breach.

Certainly, cost containment is a major reason that many companies manage situations internally for as long as possible before engaging outside counsel and experts.

However, from a control and governance standpoint, all matters involving the general counsel's office should have a client code, and such a listing should be available to the company's auditors so that all company risks are at a minimum transparent for audit purposes and subject to consideration when meeting the SEC requirements for disclosures under Item 303(a) of Regulation S-K.

Joseph J. Floyd, a CPA and attorney, is president of Floyd Advisory, a consulting firm in Boston and New York City that provides financial and accounting expertise in the areas of business strategy, valuation, SEC reporting and transaction analysis.