Strafford

Presenting a live 90-minute webinar with interactive Q&A

New SEC Guidance on Cybersecurity Disclosures: Risks, Incidents, Materiality, Data Governance Procedures

TUESDAY, JUNE 12, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Sten-Erik Hoidal, Shareholder, **Fredrikson & Byron**, Minneapolis

Timothy Newman, Partner, **Haynes and Boone**, Dallas

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-888-450-9970** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

Cybersecurity Disclosures – Lessons from SEC Guidance and the Yahoo Enforcement Action

June 12, 2018

haynesboone

Fredrikson & BYRON, P.A.

Presented by

Timothy Newman
Haynes and Boone, LLP
214.651.5029
timothy.newman@haynesboone.com

Sten-Erik Hoidal
Fredrikson & Byron, P.A.
612.492.7334
shoidal@fredlaw.com

Overview

- How did we get here?
  - 2011 Staff Guidance
  - Case studies: Target and Equifax
  - SEC enforcement prior to Yahoo: R.T. Jones and Morgan Stanley
- The 2018 Interpretive Guidance—A warning to public companies
- Yahoo—what happened and lessons learned
- Practical considerations and takeaways
  - SEC enforcement Investigations
  - Materiality determinations
  - Incident response planning and disclosure processes
  - Insider trading controls
  - Involving in-house counsel and the board
- Q&A

The SEC's 2011 Staff Guidance on Cybersecurity Disclosures

2011 Guidance – The Basics

- Issued on October 13, 2011
- Issued by SEC's Division of Corporation Finance

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

2011 Guidance – The Basics (cont.)

> For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity[1] have also increased, resulting in more frequent and severe cyber incidents.

- As a result, the Division of Corporate Finance "determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided . . . ."

2011 Guidance – Key Points

- "No existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents . . . ."
- But a number of them "may impose an obligation on registrants to disclose such risks and incidents."
- Including (potentially)
  - Risk factors – if among "most significant factors" that may make an investment speculative or risky
  - MD&A – if incident or risk is reasonably likely to have a material effect on registrant's operations, liquidity, or financial condition
  - Description of business – if incidents materially affect products, services, customer relationships, or competitive conditions
  - Legal proceedings – if in material legal proceedings relating to incident
  - Financial statement disclosures – both pre- and post-incident, if material impact on financial statements
  - Disclosure controls – if present risk to registrant's ability to process and report information required in SEC filings

Comment Letters Regarding 2011 Guidance

2011 Guidance - Comment Letters

- Expansion of risk factors, including the risk that a breach would present for a company or its products or a description of the costs and other consequences that could result from a material breach
- Clarification regarding whether a company had actually suffered a breach, including specific suggestions that a breach may have occurred
- Asked about relationships with service providers and liability a company might face in the event of a cyber attack

2011 Guidance - Comment Letters

Registrant: “Security breaches and cybersecurity threats could compromise our information.”

- SEC Staff: “Please provide a description of any cyber incidents that you have experienced that are individually, or in the aggregate, material, including a description of the costs and other consequences, and disclose the extent to which you outsource functions that have material cybersecurity risks.”

Registrant: ”Our ability to protect the confidential information of our borrowers and investors may be adversely affected by cyber-attacks.”

- SEC Staff: “Please tell us whether [your company] or its payment processing service providers would be liable to your borrowers or investors in the event that a breach occurs that could lead to the misappropriation of the clients funds from accounts linked to your platform or mobile applications. Also, tell us whether your agreements with your service providers provide for any distribution of liability in the event of a breach or other cyberattack. Review your disclosure based on your response.”

2011 Guidance - Comment Letters

Registrant: Our company faces risks “due to operational systems and technology.”

- SEC Staff: “We note your disclosure that you are exposed to operational risk, which may materialize due to a broad range of factors, including, without limitation, information technology failures, the malfunction of external systems and controls, or from external events, such as cyber-crime and fraud. Please tell us whether you have experienced cyber-crime or similar attacks in the past. For example, we note a news article published on [date] reporting that your Business On Line service remains compatible only with the Internet Explorer browser, which recently experienced security flaws. Such article also reports that “targeted attacks” exploiting such flaws have already occurred, according to Microsoft. If you have experienced cyber-crime or similar attacks, please revise your risk factor disclosure and your operational risk disclosure in future filings to disclose that you have experienced such cyber-crime or similar attacks in order to provide the proper context for your disclosure.”

Case Studies Following 2011 Guidance

Target Breach and Disclosures

- Pre-incident: March 20, 2013 10-K
  - Forward-looking risk factor disclosures
  - “If our efforts to protect the security of personal information about our guests and team members are unsuccessful, we could be subject to costly government enforcement actions and private litigation and our reputation could suffer.”
  - “A significant disruption in our computer systems could adversely affect our operations.”

Target Breach and Disclosures

- Post-incident: March 13, 2015 10-K
  - Repeated references to, and significant discussion regarding, the data breach
  - Discussion of cybersecurity and the data breach in multiple risk factors, MD&A, financial statements, etc.
- SEC investigates, but declines to bring enforcement action
  - Announced in Target's July 31, 2015 10-Q

Equifax Breach and Insider Trading

- Equifax failed to properly install a security patch to open-source software it had used
- 146.6 million individuals affected
- Four executives sold shares of Equifax days after it discovered the breach
- A committee formed to investigate the trades found no wrong doing
- The SEC charged the Company's former Chief Information Officer with insider trading
- The U.S. Attorney's Office for the Northern District of Georgia announced parallel criminal charges against former CIO

SEC Enforcement Prior to Yahoo

R.T. Jones Enforcement Action

- SEC's first ever enforcement action relating to data security
- SEC alleged R.T. Jones failed to adopt written policies and procedures designed to protect customer data as required by SEC Safeguards Rule (30(a) of Reg. S-P)
- Settlement announced on September 25, 2015, included $75,000 fine, censure, and cease-and-desist order
- Sent a clear signal that the SEC is taking cybersecurity seriously

Morgan Stanley Enforcement Action

SEC: Morgan Stanley Failed to Safeguard Customer Data

FOR IMMEDIATE RELEASE
2016-112

Washington D.C., June 8, 2016 — The Securities and Exchange Commission today announced that Morgan Stanley Smith Barney LLC has agreed to pay a $1 million penalty to settle charges related to its failures to protect customer information, some of which was hacked and offered for sale online.

The SEC issued an order finding that Morgan Stanley failed to adopt written policies and procedures reasonably designed to protect customer data. As a result of these failures, from 2011 to 2014, a then-employee impermissibly accessed and transferred the data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.

"Given the dangers and impact of cyber breaches, data security is a critically important aspect of investor protection. We expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information," said Andrew Ceresney, Director of the SEC Enforcement Division.

Morgan Stanley Enforcement Action

- An employee gained access to customers' account balances and other confidential data after discovering that that Company's authorization keys for such data were ineffective
  - The employee misappropriated customer data for 3 years
- The Safeguards Rule requires financial institutions to:
  - "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."
- According to the SEC, Morgan Stanley did not adopt procedures that could effectively protect consumer information
- Morgan Stanley agreed to pay $1 million to settle charges that it violated Rule 30(a) of Regulation S-P (the "Safeguards Rule")

The SEC's 2018 Interpretive Guidance on Cybersecurity Disclosures

2018 Interpretive Guidance – Overview

- Issued on February 20, 2018
- Unanimously approved by the Commissioners
- Acknowledged the criticality of cybersecurity and the significant risks and consequences posed by cybersecurity incidents

> Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks.

- Reinforced—and provides Commission's imprimatur on—the Division of Corporation Finance 2011 Guidance

2018 Interpretive Guidance – Overview (cont.)

- Emphasized the need to disclose cybersecurity risks to investors and provides guidelines for doing so

> Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.

- Required companies to implement controls to prevent insider trading on nonpublic information about incidents

> Additionally, directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company.

2018 Interpretive Guidance – What It Covered

- Risk Factor Disclosure
  - Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company's securities speculative or risky.

- MD&A of Financial Condition and Results of Operations
  - Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations.

2018 Interpretive Guidance – What It Covered (cont.)

- Description of Business
  - Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions.
- Legal Proceedings
  - Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings.
- Financial Statement Disclosures
- Board Risk Oversight

2018 Interpretive Guidance – What It Covered (cont.)

- Disclosure controls and procedures to evaluate effectiveness of the controls
- A company's executives must certify the design and effectiveness of disclosure controls and procedures.
- Emphasized prohibition on insider trading
- Emphasized prohibition on selective disclosure

2018 Interpretive Guidance – What It Did Not Cover

Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures

Commissioner Kara M. Stein

Feb. 21, 2018

Yesterday, the Commission attempted to tackle an increasingly important issue: How should a public company tell its investors about its cybersecurity risks and incidents?[1]

Undeniably, the high-profile data losses and security breaches that have occurred across the public and private sectors show that no company or organization is immune from cyberattack. Unfortunately, one only need look back to the past eight years to see example after example of these attacks. In 2010, a sophisticated cyberattack affected more than 75,000 computer systems at nearly 2,500 companies in the United States and around the world.[2] In 2014, hackers broke into the computer systems of a major Hollywood studio, stealing confidential documents and exposing these documents and other personal information to potential cybercriminals.[3] And last year, we learned that a major cybersecurity breach at a public company may have potentially affected half of the U.S. population.[4] When the magnitude of the breach was revealed publicly, the company's stock price plummeted, losing over $5 billion in market value.[5]

- Consequences of failure to heed the guidance
- Specific improvements to cybersecurity risk management
- Minimum standards for protection of personally identifiable information
- Requiring companies to notify investors of cyber incident within a certain time frame

2018 Interpretive Guidance – Commission(er) Statements

- SEC Chairman Clayton released a statement that underscored the purpose of the guidance:
  - to "promote clearer and more robust disclosure by companies about cybersecurity risks and incidents" and make more complete information available to investors
- But was met with criticism from other commissioners
  - SEC Commissioner Kara Stein released a statement expressing her "disappoint[ment] with the Commission's limited action"
  - In her words, "we could have helped companies formulate more meaningful disclosure for investors. Instead, yesterday's guidance provides only modest changes to the 2011 staff guidance."
- Takeaway: <u>there is more to come</u>

Case Study: The SEC's Enforcement Action Against Yahoo/Altaba

Yahoo/Altaba – The Background

Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million

FOR IMMEDIATE RELEASE
2018-71

Washington D.C., April 24, 2018 — The Securities and Exchange Commission today announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts.

Yahoo/Altaba – The Background

- Yahoo's information security team learned that hackers had stolen usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts.

- The information security team reported this to Yahoo's senior management and legal teams.

Yahoo/Altaba – The Background

- Despite this knowledge, Yahoo allegedly failed to acknowledge this breach in risk factor disclosures in annual reports and quarterly reports in the succeeding years.

- In negotiations with Verizon, Yahoo allegedly falsely represented that it was only aware of four minor data breaches.

Yahoo/Altaba – The Settlement

- Announced on April 24, 2018
- First ever enforcement action re: cybersecurity disclosures
- Yahoo agreed to
  - a $35 million penalty
  - cease-and-desist from violations of Securities Act and Exchange Act
  - cooperate w/ SEC's other proceedings and further investigation, including securing employee participation
  - provide documents and materials as SEC may request
- Yahoo did not admit or deny SEC's allegations

Yahoo/Altaba – The Settlement

The SEC's cease-and-desist order found that Yahoo:

- Knew of a massive 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
  - Risk factor disclosures were forward-looking only and did not disclose information pertaining to the actual breach
  - MD&A omitted trends or uncertainties regarding liquidity/net revenue
  - Disclosure controls and procedures were not effective
- Violated the Securities Act (17(a)(2) and 17(a)(3)), the Exchange Act (13(a)), and multiple rules

Yahoo/Altaba – The Settlement

Highlights from the cease-and-desist order and announcement

1. Misrepresentations contained in purchase agreement with Verizon and filed w/ SEC found to violate disclosure obligations
2. Placed blame squarely on senior management and in-house legal counsel
   - "[D]id not properly assess the scope, business impact, or legal implications of the breach"
   - "[D]id not share information regarding the breach with Yahoo's auditors or outside counsel"
3. "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.

Yahoo/Altaba – The Lessons

- Ensure complete investigation and analysis of cyber events
- Make sure the results of any investigation are effectively communicated across the organization
- Make sure your disclosure process includes consideration of cyber events
- Disclosure of a cyber risk only may be misleading if a breach has actually occurred
- The SEC will look at more than just a company's Forms 10-K and 10-Q for misleading disclosures

Yahoo – Securities Class Action

- January 2017 – First of several securities class actions relating to two Yahoo breaches filed
- Plaintiffs alleged
  - Yahoo made materially false/misleading statements in SEC filings from 2013-2016
  - Plaintiffs lost money on their investment when the company's stock value declined following disclosure and subsequent renegotiation of Verizon purchase price
- March 5, 2018 – Settlement reached
  - $80 million to class
  - Plaintiffs' counsel to seek up to $20 million

Yahoo – Securities Class Action (cont.)

- Why is the Yahoo security class action significant?
  - First major recovery in a shareholders' suit relating to a cybersecurity incident
  - First securities class actions to be filed based on a cybersecurity incident (pivot from prior shareholder derivative cases)
- Does this mean a flood of securities class actions relating to public company cybersecurity incidents?
  - Not a flood (but maybe a small creek)
  - Some new life breathed into shareholder suits

Practical Considerations

Practical Considerations – SEC Enforcement Investigations

- The general process:
  - Tip or complaint
  - Formal order
  - Subpoenas for documents
  - Subpoenas for testimony
  - Enforcement decision
  - If necessary, Wells process
  - If necessary, settlement or litigation

- Investigations often last years, can be costly, and can be disruptive to a business

Practical Considerations – Materiality

- Importance of any compromised information
- Impact of the incident on the company's operations
- Range of harm that such incidents could cause, such as harm to reputation, financial performance, and customer and vendor relationships
- Possibility of litigation or regulatory investigations or actions

Practical Considerations – Controls and Procedures

What do public companies need?

- A formalized, comprehensive information security program that incorporates disclosure controls
  - Per the guidance, those controls must allow the company to assess the significance of risks/incident, analyze their impact on a company's business, and engage in appropriate communications
  - Critically, the controls must ensure that relevant information is gathered and presented to management or responsible persons for decisions regarding disclosure to investors

Practical Considerations – Controls and Procedures

What does that mean (as a practical matter)?

- Communication between the relevant groups in advance of SEC filings
  - Implement a standardized process for communication between stakeholders—e.g., information security, incident response, legal, and management—about cyber incidents and risks in advance of disclosures
- An analysis of disclosure requirements as part of the incident response plan
  - Include trigger re: disclosure to the SEC/investors
  - Designate incident response team member to own the issue (e.g., coordinate resources and facilitate dialog)

Practical Considerations – Insider Trading Policies

- Cross-reference to incident response plans
- Conduct training to ensure awareness of insider trading concerns among your IT and other personnel who may have access to information regarding potentially material cyber events
- Consider a blackout period when a potentially material cyber event has been discovered
- Don’t forget about Regulation FD, which generally precludes selective disclosure of material non-public information

Practical Considerations – Board-Level Involvement

What should bards be doing?

- Oversee cybersecurity risk management like other enterprise-wide risks
- Assure themselves that the necessary procedures, staff, and resources are in place to address cyber risk, including risks relating to disclosures
- Ask appropriate questions and watch for red flags
- Set appropriate expectations for management to implement/update controls and procedures for cybersecurity disclosures

Practical Considerations – In-House Legal Counsel

- Make sure that cyber risks and incidents are evaluated in connection with SEC filings
- Review incident response plan to ensure all disclosure obligations are accounted for
  - Note the importance of assessing the scope, business impact, and legal implications of a breach in determining whether to disclose
- As part of incident response, include a review of prior SEC filings for necessary corrections/updates
- Use outside counsel (or auditors) as a check on SEC disclosures

Thank You

Timothy Newman
Haynes and Boone, LLP
214.651.5029
timothy.newman@haynesboone.com

Sten-Erik Hoidal
Fredrikson & Byron, P.A.
612.492.7334
shoidal@fredlaw.com