ALSTON & BIRD

WWW.ALSTON.COM

Securities Litigation / Cybersecurity Preparedness & Response / Securities Law / ADVISORY ■

FEBRUARY 27, 2018

SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures

by Cara Peterman, Lauren Tapson Macon, and Hillary Li

The Securities and Exchange Commission (SEC) issued a press release announcing its unanimous approval of a statement by SEC Chairman Jay Clayton and interpretive guidance (the "2018 Guidance") to assist public companies in preparing disclosures about cybersecurity risks and incidents. This is the first interpretive guidance published by the full Commission on the topic of cybersecurity for public companies, and it may foreshadow increased SEC action to protect investors from the potential negative effects of increasingly common large-scale data breaches. The 2018 Guidance formalizes and expands on the SEC staff's earlier position that cybersecurity risks and incidents may trigger disclosure obligations for public companies. In addition, the 2018 Guidance focuses on (1) the importance of comprehensive cybersecurity policies and procedures that enable public companies to understand the impact and materiality of cybersecurity incidents and facilitate the timely disclosure of such incidents; and (2) the prevention of insider trading in connection with cybersecurity incidents.

In 2011, the SEC's Division of Corporation Finance released CF Disclosure Guidance: Topic No. 2 (the "2011 Guidance"), addressing the staff's views that companies may be required to disclose cybersecurity risks and incidents as part of their existing disclosure obligations. Since 2011, the SEC has issued intermittent informal statements relating to cybersecurity, including in connection with its Cybersecurity Roundtable in 2014 and Chairman Clayton's September 2017 Statement on Cybersecurity, which disclosed an intrusion into the SEC's own data systems. Given the SEC's public focus on cybersecurity issues, it has long been expected that the SEC would issue more formal guidance.

In many respects, the 2018 Guidance varies little from the 2011 Guidance and addresses disclosure issues that most public companies have already integrated into their disclosure processes. Among other things, the 2018 Guidance reinforces that companies should consider the materiality of cybersecurity risks and incidents when preparing disclosures.

The 2018 Guidance, however, does provide a more comprehensive and detailed view of the SEC's expectations for public company disclosures. Though the SEC does not expect disclosures to detail circumstances that could "provid[e] a 'roadmap' for those who seek to penetrate a company's security protections," the SEC does expect companies to

make tailored disclosures of cyber risks and incidents that are material to investors, including the associated financial, legal, or reputational consequences of a significant breach. The 2018 Guidance repeatedly emphasizes that required disclosures should be made "timely" and on an ongoing basis. For example, while the SEC understands that some material facts may not be available at the time of the initial disclosure, it emphasizes that "an ongoing internal or external investigation … would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." Companies may also have a duty to correct or update a prior disclosure of a cybersecurity risk or incident in certain circumstances.

The 2018 Guidance adds specific requirements and suggestions for companies to the 2011 Guidance:

- Risk factor disclosures should take into consideration past incidents involving "suppliers, customers, competitors, and others" and should include cybersecurity risks "that arise in connection with acquisitions."

- To the extent cybersecurity risks are material to a company's business, the company's proxy statement disclosure regarding the board's oversight of risk should include the nature of the board's role in overseeing cybersecurity risks in particular.

- Companies should assess whether their disclosure controls and procedures relating to cybersecurity ensure that relevant information is reported "up the corporate ladder to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on" material nonpublic information about cybersecurity.

- Executive management certifications regarding the design and effectiveness of disclosure controls and procedures should consider whether cybersecurity risks and incidents pose a risk to the company's ability to gather and report information for SEC filings and whether such deficiencies would render disclosure controls and procedures ineffective.

- Companies should consider how their code of ethics and insider trading policies take into account and prevent insider trading related to cybersecurity risks and incidents, and whether trading restrictions may be appropriate for insiders while companies are investigating and assessing significant cybersecurity incidents.

- Companies are expected to have policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively in violation of Regulation FD.

The 2018 Guidance is effective upon publication in the *Federal Register*, which typically occurs within 4–7 days of release. Although most of the topics covered in the 2018 Guidance will not come as a surprise to public company counsel, officers, and directors, it is somewhat unsettling that the release of the SEC's formal views on these topics comes while most public companies are finalizing their annual reports. Moreover, several focal points of the 2018 Guidance, such as timely disclosure, insider trading, executive management certifications, and the admonition that the SEC is carefully monitoring cybersecurity disclosures, in combination with the SEC's recent investigations arising out of the data breaches at Equifax Inc. and Yahoo Inc., suggest that the SEC will not soon divert its attention—and its investigative and enforcement powers—from the cybersecurity arena.

You can subscribe to future ***Securities Litigation*** advisories, ***Cyber Alerts***, ***Securities Law*** advisories, and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

Securities Litigation

Lisa R. Bugni
404.881.4959
lisa.bugni@alston.com

Gidon M. Caine
650.838.2060
gidon.caine@alston.com

Charles W. Cox
213.576.1048
charles.cox@alston.com

Mary C. Gill
404.881.7276
mary.gill@alston.com

Susan E. Hurd
404.881.7572
susan.hurd@alston.com

Brett D. Jaffe
212.210.9547
brett.jaffe@alston.com

John A. Jordak, Jr.
404.881.7868
john.jordak@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Robert R. Long
404.881.4760
robert.long@alston.com

Paul Monnin
404.881.7394
paul.monnin@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

Theodore J. Sawicki
404.881.7639
tod.sawicki@alston.com

Cybersecurity Preparedness & Response

Jim Harvey
404.881.7328
jim.harvey@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Securities Law

David A. Brown
202.239.3463
dave.brown@alston.com

Lesley Solomon
404.881.7364
lesley.solomon@alston.com

Julie Mediamolle
202.239.3702
julie.mediamolle@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333