HAWKINS ADVISORY

CYBERSECURITY

Introduction

This Advisory describes recent developments regarding disclosure of cybersecurity[1] risks and incidents and their import for municipal disclosure.

The Securities and Exchange Commission (the "SEC") recently published interpretive guidance (the "2018 Guidance") to assist public companies (i.e., those companies subject to registration with the SEC) in preparing disclosures about cybersecurity risks and incidents.[2] The 2018 Guidance updated guidance provided in 2011 by the Staff of the SEC's Division of Corporation Finance.[3] In each guidance, the SEC did not mandate any particular disclosure, but rather advised registrants to consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements and periodic and current reports. Although each guidance was directed to corporate SEC registrants, these guidances are also relevant to municipal issuers.[4] The general antifraud rules[5] apply to all securities disclosure, regardless of whether the related security is exempt from SEC registration. In addition, last month, in an administrative proceeding dated April 24, 2018 (the "Yahoo Enforcement Action"), the SEC found that Yahoo's risk factor disclosures in its annual and quarterly reports from 2014 through 2016 were materially misleading in not disclosing a massive data breach that had occurred in 2014.[6]

Recently, there have been significant cybersecurity incidents affecting municipal agencies, including a freezing of systems of the City of Atlanta; an attack on Baltimore's 911 system; an attack on the Colorado Department of Transportation's computers; and a closing of the Port of Los Angeles's largest terminal.[7] Municipal agencies, similar to other business entities, face significant risks relating to the use and application of computer software and hardware.

Set forth below is a summary of the 2018 Guidance and the Yahoo Enforcement Action, and questions for consideration regarding cybersecurity risks and incidents in the municipal context.

The 2018 Guidance

The 2018 Guidance states the following:

> In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information on the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.
>
> 2018 Guidance, pp. 10-11 (footnotes omitted)

The 2018 Guidance further noted that "[c]ompanies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors."

The 2018 Guidance identified the following issues, among others, in evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;

[1] The SEC Staff, in its 2011 guidance, cited the "Whatis?com" website for its definition of cybersecurity, which currently reads: "the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."

[2] SEC Rel. Nos. 33-10459, 34-82746 (Feb. 21, 2018).

[3] CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

[4] "Municipal issuers," as used in this Advisory, also includes "obligated persons" as defined in SEC Rule 15c2-12.

[5] Section 10(b) and Rule 10b-5 of the Securities Exchange Act of 1934 and Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933.

[6] *In re* Altaba Inc. f/d/b/a Yahoo! Inc., SEC Rel. Nos. 33-10485, 34-83096 (Apr. 24, 2018).

[7] *Hacking Threat comes into Focus for Municipal Finance,* THE BOND BUYER, May 3, 2018.

- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

The Yahoo Enforcement Action

In late 2014, Yahoo incurred "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."[8] Despite such knowledge, Yahoo did not include information regarding the breach in its annual and quarterly filings from 2014 through 2016.

In the summer of 2016, Yahoo was engaged in negotiations with Verizon Communications, Inc. ("Verizon") regarding the sale of Yahoo's operating business, and an agreement was reached on July 23, 2016. During the course of the negotiations, Verizon had made inquiries of Yahoo regarding past data breaches, but Yahoo did not disclose the 2014 data breach to Verizon or to the public until September 2016. After such disclosure, Verizon renegotiated the stock purchase agreement to reduce the purchase price by 7.25%.

Yahoo had been making generic risk disclosure in 2014-2016 regarding only *potential* data breaches even after it was aware of an *actual* massive data breach that occurred in late 2014. But as the SEC noted in the 2018 Guidance, such generic disclosure may not be sufficient: "if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur." In addition, the SEC noted that Yahoo's senior management and legal teams did not share information regarding the breach with Yahoo's auditors or outside counsel in order to assess the company's disclosure obligations in its public filings. The SEC further noted that Yahoo did not maintain disclosure controls and procedures designed to ensure that reports from Yahoo's information security team were timely shared with responsible officials.

The SEC found that Yahoo violated Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 (negligence standard, in connection with materially misleading disclosure). Yahoo paid a civil money penalty of $35 million.

Municipal Securities Disclosure

Disclosure by municipal issuers of cybersecurity risks and incidents is governed by the same guidelines and standards that apply to municipal disclosure generally – namely, what is material to an investor regarding the particular securities being offered. The following are questions that may be asked to aid in analyzing whether disclosure of cybersecurity risks or incidents is appropriate:

Cybersecurity Incidents

- Has a cybersecurity incident[9] occurred within the last five years?
- Was such incident unintentional or deliberate?
- Was such incident the result of attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and "hacktivists"?
- Have the security flaws been corrected?
- What were the remediation costs? Liability amounts?
- What are the increased cybersecurity protection costs (including additional personnel, training employees, and engaging third party experts and consultants)?
- Is the issuer currently subject to litigation, regulatory investigation, or remediation costs associated with a cybersecurity incident?

Even if there have been no cybersecurity incidents, disclosure may be appropriate if a risk of such incidents exists. The SEC noted in the 2018 Guidance:

> 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

[8] Yahoo Enforcement Action.

[9] The 2018 Guidance, at fn. 3, quotes from the U.S. Computer Emergency Readiness Team website in defining "cybersecurity incident" as follows: "[a]n occurrence that actually or potentially results in adverse consequences to . . . an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences."

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.[10]

Cybersecurity Risks

- Is the issuer (obligated person) particularly vulnerable to, or attractive as a target for, cybersecurity attacks?
  - Hospitals and health systems have suffered data breaches
  - Municipal utilities have made payments to regain access to their systems
  - Power supply systems and infrastructure generally may be vulnerable to cybersecurity attacks
- Is the issuer subject to regulatory requirements?
  - S&P notes that the North American Electric Reliability Organization establishes and polices cybersecurity standards for electric utilities[11]
- Has the issuer established cybersecurity risk management policies and procedures and conducted associated training regarding cybersecurity risks and incidents?
- Has the issuer analyzed the probability and potential magnitude of cybersecurity incidents?
- Does the issuer carry insurance against cybersecurity incidents? What is the coverage provided?
- Is the issuer vulnerable to risks of cybersecurity attacks on third-party supplier and service providers?

Conclusion

The SEC has provided interpretive guidance to public companies regarding the disclosure of cybersecurity risks and incidents, and has brought its first enforcement action for misleading disclosures regarding such issues. The general antifraud provisions that govern securities disclosure are the same for a public company and a municipal issuer. Accordingly, the SEC's 2018 Guidance and the Yahoo Enforcement Action deserve careful consideration in the context of a municipal securities offering, and the questions identified above are intended to aid in such analysis.

[10] 2018 Guidance, p.4.

[11] S&P Credit FAQ: "Cybersecurity, Risk, and Credit in U.S. Public Finance" (Mar. 13, 2017).

New York
7 World Trade Center
250 Greenwich Street
New York, NY 10007
Tel: (212) 820-9300

Washington, D.C.
601 Thirteenth Street, N.W.
Washington, D.C. 20005
Tel: (202) 682-1480

Newark
One Gateway Center
Newark, NJ 07102
Tel: (973) 642-8584

Hartford
20 Church Street
Hartford, CT 06103
Tel: (860) 275-6260

Ann Arbor
2723 South State Street
Ann Arbor, MI 48104
Tel: (734) 794-4835

Sacramento
1415 L Street
Sacramento, CA 95814
Tel: (916) 326-5200

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071
(213) 236-9050

San Francisco
One Embarcadero Center
San Francisco, CA 94111
Tel: (415) 486-4200

Portland
200 SW Market Street
Portland, OR 97201
Tel: (503) 402-1320

Hawkins DELAFIELD & WOOD LLP