Alert

December 7, 2023

COZEN O'CONNOR

Cybersecurity Disclosure Guidance for Municipal Bonds

Cyberattacks against municipal entities and 501(c)(3) organizations are becoming increasingly sophisticated and severe. The potential impact of these cyberattacks on entities is significant in both the time required to address the impact of the attack and the costs of any liability and remediation. Credit rating agencies have emphasized that cyberattacks pose a credit risk to municipal bond issuers and may result in a lower credit rating, which increases borrowing costs.

On July 26, 2023, the Securities and Exchange Commission (the SEC) adopted final rules (the Rules) requiring public companies to disclose material cybersecurity incidents and to annually disclose material information regarding their cybersecurity risk management, strategy, and governance.[1] Although the Rules only apply to public companies subject to the reporting requirements of the Securities Exchange Act of 1934, the SEC has frequently urged the municipal markets to look to the disclose requirements imposed on public companies. Accordingly, the Rules provide guidance to municipal issuers and 501(c)(3) organizations on how they may consider disclosing cybersecurity matters in offering documents and on the formulation of policies and strategies to combat cyberattacks.

Disclosure of a Material Cybersecurity Incident

Commencing on December 18, 2023, the Rules require public companies to publicly disclose any "cybersecurity incident" they determine to be material and describe the material aspects of its

1. nature, scope, and timing; and
2. impact or reasonably likely impact on the company, including its financial condition and results of operations.

A "cybersecurity incident" is defined as "an unauthorized occurrence on or conducted through a [company's] information systems that jeopardizes the confidentiality, integrity, or availability of a [company's] information systems or any information residing therein." The Rules emphasize that the term "cybersecurity incident" is to be construed broadly.

Disclosure of a cybersecurity incident will generally be due within four business days after the affected company determines that a cybersecurity incident is material.[2] This requirement is similar to the disclosure of certain reporting events the municipal market is accustomed to under Rule 15c2-12.[3]

Annual Disclosure

In addition, commencing with its annual report for the fiscal year ending on or after December 15, 2023, public companies will be required to provide annual disclosures related to the companies' processes for the management and governance of cybersecurity threats.

In the annual disclosure, companies must describe the following:

1. The process, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, the company should address:
    i. whether and how any such processes have been integrated into the company's overall risk management system or processes;
    ii. whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
    iii. whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

Scott R. Mehok

Member

smehok@cozen.com
Phone: (717) 773-4209
Fax: (717) 703-5901

Related Practice Areas

- Capital Markets & Securities
- Public & Project Finance

2. Whether any risks related to cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition, and if so, how.
3. The board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.
4. The management's role in assessing and managing the company's material risks from cybersecurity threats, including:
    i. whether and which management positions or committees are responsible for assessing and managing such risks and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
    ii. the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
    iii. whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Guidance for Municipal Market Participants

Although the municipal market is not subject to Rules, they offer helpful insight and guidance to its participants. The Rules provide municipal issuers and 501(c)(3) organizations with a valuable framework for drafting cybersecurity risk disclosure in offering documents. Additionally, the Rules provide guidance on drafting and implementing policies and procedures for responding to cyberattacks.

---

[1] SEC Release Nos. 33-11216 and 34-97989.

[2] The cybersecurity incident disclosure may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

[3] 17 CFR § 240.15c2-12.