Bond Case Briefs

Municipal Finance Law Since 1971

Three Takeaways for Municipal Bond Issuers From the New SEC Cybersecurity Disclosure Rules: McGuireWoods

State and local governments increasingly are becoming targets of cybersecurity attacks. According to CloudSEK, cyberattacks targeting the government sector increased by 95% worldwide in the second half of 2022, compared to the same period in 2021. With the rise of cybersecurity threats, S&P Global Ratings, a leading rating agency, noted that cyberattacks pose a growing credit risk to municipal bond issuers and warned that weak cybersecurity could lead to credit downgrades over the next 12 months.

With the increased scrutiny on cybersecurity by S&P and the growing threat of cyberattacks, disclosure about cybersecurity risk has become increasingly common for municipal bond issuers. To date, there is no official guidance from the U.S. Securities and Exchange Commission (SEC) about inclusion of information on cybersecurity risks for municipal bond issuers.

This lack of official guidance is due in part to the SEC's limited ability to directly regulate municipal bond transactions. The SEC has indicated that many principles applicable to the registered market can be applied to the municipal market. Many municipal issuers also rely on guidance from the registered market when analyzing disclosure issues. Recent SEC rulemaking on cybersecurity disclosure is one instance where municipal issuers can apply these principles.

On July 26, 2023, the SEC adopted a final rule standardizing cybersecurity disclosure practices for public companies that offers guideposts for municipal issuers on disclosure about cybersecurity. Beginning in December 2023, public companies will have to make a timely materiality determination about cybersecurity incidents and, if an incident is determined to be material, disclose the same within four business days of such determination. Importantly, the SEC provided that an item is material if there is a "substantial likelihood that a reasonable shareholder" would deem the information meaningful to make an investment decision. Once a material cybersecurity incident determination is made, the company must disclose within four business days: (1) the nature, scope and timing of the cybersecurity incident; and (2) the incident's qualitative and quantitative impact (or the reasonably likely impact) on the company, including, but not limited to, its financial condition, operations, reputation and relationships.

Additionally, beginning with its annual report for the fiscal year ending on or after Dec. 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 (1) the process for the assessment, identification and management of risks for cybersecurity threats; (2) whether any risks related to cybersecurity have materially affected (or are reasonably likely to materially affect) their business strategy, operations or financial conditions; and (3) the board's oversight and management of cybersecurity risks.

Although municipal bond issuers will not be required to comply with the new SEC rules, the rules provide valuable guidance for issuers on how to address cybersecurity risks in their disclosure documents and through cyberattack policies. In applying the principles found in the new rules,

municipal bond issuers should make the following key considerations:

Implement and regularly reassess cybersecurity policies.

Municipalities are vulnerable to cybersecurity attacks without the proper assessment, response and management policies. An issuer that does not have a formal cybersecurity policy should consider developing a framework related to cybersecurity preparedness to institute centralized responsibilities and a transparent strategy on how to proceed if cybersecurity incidents occur. Even issuers that have formal policies should regularly reassess their policies to ensure the practices are up to date.

To create a workable policy, municipal bond issuers should consider the risks unique to their particular infrastructure and how to best protect their financial condition, operations, reputation and relationships. Municipalities also should consider whether cybersecurity insurance could be managed through an insurance policy as part of their overall risk management system.

For all issuers, ongoing management of cybersecurity risks through regular weakness testing will ensure that municipalities have an action plan in the event of a real cybersecurity attack.

Prepare a disclosure that addresses cybersecurity policy and procedures and material prior attacks.

Including cybersecurity attacks as a risk factor in offering document disclosure has become a best practice to address rating agency and investor questions. In preparing disclosures, issuers should consider their current risk posture, including policies and procedures for cybersecurity risk management, any past cybersecurity attacks and to what degree the board oversees this or delegates to management the day-to-day risk management. Issuers should work closely with legal counsel to craft disclosures on these points.

Disclosures still should be guided by materiality.

While the SEC has been reluctant to define “materiality,” the new rules for the registered market demonstrate that disclosures regarding cybersecurity (as with most disclosure issues) should revolve around materiality. In response to comments from the market during the rulemaking process, the final rule requires disclosure of “management’s role in assessing and managing the registrant’s material risks from cybersecurity threats.”

Further, the adopting release notes that certain actions are material by virtue of the level of attention provided by the board of directors and management. The final rule does not contain a materiality qualifier related to the requirement that registrants describe the oversight undertaken by their board of directors and any applicable committee responsible for this oversight because, by virtue of the board or a committee taking an active role in oversight, the SEC deemed that material to investors.

McGuireWoods LLP – Anna C. Horevay, Thomas William Bruno and Camille A. Pappy

September 6 2023