Bond Case Briefs

Municipal Finance Law Since 1971

What All Municipal Bond Issuers Should Know About Cybersecurity Risk Disclosure in 2024.

Over the last fifteen years, the Securities and Exchange Commission (SEC) has increased its focus on inadequate disclosure relating to governmental debt issues. Although municipal bond issuers are largely exempt from federal requirements for securities, they are required to comply with the antifraud provisions of the Securities Act of 1933 and Rule 10b-5 of the Securities Exchange Act of 1934 (the Exchange Act). These laws prohibit the making of material misstatements, or omissions of material facts if those facts are necessary to avoid a misleading statement. Issuers who fail to comply with disclosure requirements may be subject to regulatory actions and/or monetary fines. Primary market disclosure practices for municipal securities have developed as a result of these antifraud provisions and the regulatory actions brought by the SEC.

Cybersecurity Risk Disclosure

With a drastic increase in cyberattacks impacting municipal governments and the increased scrutiny on cybersecurity by rating agencies, cybersecurity risk disclosure has become increasingly more important for municipal bond issuers. There is no official guidance from the SEC about what municipal bond issuers should disclose about cybersecurity risks. The SEC has indicated that many principles applicable to the registered market provide guidance and can be applied to the municipal market.

1. On July 26, 2023, the SEC adopted a new rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Exchange Act (the "Final Rule"). In summary, the Final Rule requires: disclosure of material cybersecurity incidents within four (4) business days of the company's determination that the cybersecurity incident is material;
2. new annual disclosures regarding the company's cybersecurity risk management and strategy, including with respect to the company's processes for managing cybersecurity threats and whether risks from cybersecurity threats have materially affected the company; and
3. new annual disclosures regarding the company's cybersecurity governance, including with respect to oversight by the board and management.

Best Practices for Municipal Bond Issuers

Although municipal bond issuers are not required to comply with the Final Rule, it provides guidance to municipal bond issuers in preparing cybersecurity risk disclosure. Such issuers should consider the following points for inclusion in their disclosures:

1. Cybersecurity attacks, if material;
2. Existence and description of policies and procedures for cybersecurity risk management;
3. In the absence of a formal policy, develop a framework related to cybersecurity preparedness to institute centralized responsibilities and a transparent strategy on how to proceed if cybersecurity incidents occur;

4. How and when the policies are reassessed to ensure the practices are up to date;
5. Note the risks unique to the particular infrastructure and how to best protect the issuer's financial condition, operations, reputation and relationships;
6. Existence of cybersecurity insurance, what it covers and the deductible.

Pullman & Comley, LLC

by Jessica Grossarth Kennedy

January 18, 2024