Bond Case Briefs

Municipal Finance Law Since 1971

The SEC's Proposed New Cybersecurity Disclosure Requirements for Public Companies: What Do They Mean for Municipal Issuers and Borrowers? - Orrick

- Governmental entities have increasingly experienced cybersecurity incidents impacting their operations and finances over the last few years, with some breaches costing upwards of $40 million.
- Many issuers and borrowers of municipal bonds are taking steps to defend themselves against such attacks, and may also need to determine how and when to disclose such efforts and any material cybersecurity incidents to the municipal market.
- While the SEC's recently proposed disclosure rules for public companies regarding cybersecurity incidents and related policies do not apply to municipal issuers and borrowers (unless the borrower is a public company) and are not final, they do provide helpful context and guidance for how the SEC may view cybersecurity disclosures in the municipal market.

In light of these considerations, issuers and borrowers in the municipal market should:

- Review the SEC's proposed cybersecurity disclosure rules and their implications for the municipal market, specifically around incident reporting and periodic disclosure of risk management, strategy, and governance.
- Focus on their own cyber defenses and mitigation strategies, since this has been a particular focus of rating agencies on public companies when assessing the strength of a particular credit.

A Growing Problem

In recent years, governmental entities have increasingly experienced cybersecurity incidents impacting their operations and finances. According to a white paper published by KnowBe4 in 2020, the median cost of a data breach for a state was $1.87 million, with some breaches costing upwards of $40 million. Many issuers and borrowers of municipal bonds ("issuers and borrowers") are taking steps to defend themselves against such attacks. They may wonder how and when to disclose such efforts and any material cybersecurity incidents to the municipal market.

The SEC has proposed new disclosure rules for public companies regarding cybersecurity incidents and related policies and procedures. Since the SEC does not have the power to adopt similar rules for issuers and borrowers (unless the borrower is a public company), the proposed rules **do not** apply to issuers and borrowers. They do, however, provide useful context and guidance for how the SEC may view cybersecurity disclosures in the municipal market, specifically around incident reporting and periodic disclosure of risk management, strategy, and governance.

Our governance and data privacy teams published an article summarizing the proposed rules as applied to public companies generally and proposing steps public companies could consider taking now. Our public finance and data privacy teams have prepared this supplement to that article, summarizing the key takeaways for issuers and borrowers. **We encourage you to read this supplement together with the underlying article.**

Applying the SEC's Proposed Rules to the Municipal Market

The SEC's proposed rules fall into two categories: (1) incident reporting; and (2) periodic disclosure of cybersecurity risk management, strategy, and governance. We will treat each category separately.

Incident Reporting

Public Company Rules: The SEC's proposed rules reveal its focus on timely disclosure of material cybersecurity incidents on a public company's Form 8-K by requiring that material cybersecurity incidents are reported within four business days from the materiality determination.

The SEC's proposed rules do not provide specific guidance for what constitutes a material cybersecurity incident. They do provide that the required timing of a public company's Form 8-K filing is tied to the company's determination that the incident is material rather than to its discovery of the underlying incident.

Additionally, the requirement applies to compromises of the company's "information system," which includes systems owned or used by the public company and may include third-party information resources such as cloud infrastructure and service providers.

Finally, the SEC's proposed rules require periodic updates reflecting material changes or additions to previously disclosed incidents. That would include information regarding remediation.

Application to the Municipal Market: In the municipal market context, the disclosure analogue for a public company's Form 8-K is an issuer or borrower's material event notice filed pursuant to its continuing disclosure undertakings and SEC Rule 15c2-12.

Rule 15c2-12 does not specifically require issuers and borrowers to disclose material cybersecurity incidents. Such entities may disclose incidents through voluntary event notices on the MSRB's Electronic Municipal Market Access ("EMMA") website.

In addition, when issuers and borrowers speak to the market through offering documents,[1] quarterly and/or annual continuing disclosure reports, or other communications, they may want to consider disclosing recent material cybersecurity incidents. Issuers and borrowers may also want to consider focusing on developing and/or improving internal reporting systems to facilitate the discovery of and determinations of materiality regarding internal and third-party cybersecurity incidents.

Issuers and borrowers may want to consider the following questions when developing and/or improving reporting systems relating to cybersecurity incidents:

- Do you have a current and tested incident response plan?
- Do you have cybersecurity policies and procedures in place that require employees to quickly escalate cybersecurity incidents to those empowered to make materiality and disclosure determinations?[2]
- Do you have a process in place to assess the range and magnitude of financial impacts of a cybersecurity incident, as they become available, and memorialize materiality determinations?
- Do your contracts with third parties that make up your "information system" provide for incident reporting and the cooperation necessary to make materiality and disclosure determinations regarding third-party cybersecurity incidents?
- Do you have a process in place to track updates regarding previously disclosed cybersecurity incidents and provide such updates to those empowered to make materiality and disclosure determinations?

- Have you discussed with bond or disclosure counsel the implications of any cybersecurity incidents and possible voluntary disclosures?

Periodic Disclosure of Risk Management, Strategy, and Governance

Public Company Rules: The SEC's proposed rules also reveal a focus on public companies' internal risk management, strategy, and governance. Specifically, the proposed rules include changes to Regulation S-K, and corresponding changes to Form 10-K and Form 10-Q to require additional disclosures.

The proposed rules would require a public company to periodically disclose information about the processes of its board of directors and key management relating to cybersecurity issues. Specifically, the SEC proposes disclosure relating to "whether or how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight." The agency would also require disclosure of whether or not a company has a Chief Information Security Officer (including that person's background and reporting line). In addition, the SEC's proposed rules require a public company to periodically disclose whether any members of its board have expertise in cybersecurity, and to provide detail regarding the nature of that expertise. The SEC's proposed rules reveal its increasing desire to obtain detailed and specific disclosures regarding a public company's internal processes and expertise relating to cybersecurity.

Application to the Municipal Market: In the municipal market context, the disclosure analogue for a public company's Form 10-K and Form 10-Q is an issuer or borrower's annual report and quarterly report (if any), respectively, filed pursuant to its continuing disclosure undertakings. As with cybersecurity incident reporting, there is no specific requirement that issuers and borrowers include in annual or quarterly reports information regarding internal risk management, strategy, and governance. However, given the SEC's marked focus on cybersecurity-related disclosure (including the two SEC enforcement actions in 2021 relating to data privacy incidents referenced in footnotes 1 and 2), issuers and borrowers may want to evaluate the quality of their disclosures in this area whether through voluntary event filings, annual and/or quarterly continuing disclosure reports, offering documents, or other communications to the market.

More broadly, issuers and borrowers should review and update their cybersecurity policies and disclosure procedures. They may also want to focus on developing disclosures relating to existing cybersecurity policies and procedures they can update and adapt for quarterly and annual reports and offering documents. Given the SEC's focus on the expertise of individual directors or employees, issuers and borrowers may also consider collecting information regarding cybersecurity expertise that members of their governing bodies and key staff members possess and consider whether an internal Chief Information Security Officer position exists or can be created. In undertaking such efforts, we recommend that issuers and borrowers consider the following questions:

- Do you have comprehensive information security policies
- Have you had any privacy or security incidents that involve confidential or personal data?
- How does your governing body evaluate cybersecurity risk and what role does cybersecurity risk play in its decision-making process?
- Do you have a Chief Information Security Officer, or other individual designated as responsible for information security?
- Which members of your governing body and staff, including the Chief Information Security Officer, if any, possess expertise relating to cybersecurity matters?
- Do you have cyber insurance, and if so, what does it cover and what are the retention and limits?
- Do you conduct periodic risk assessments, and if so, have any identified risks been remediated or added to a security roadmap?

- Have there been any third-party security assessments, and if so, have the identified issues been remediated or added to a security roadmap?

Additional Considerations for the Municipal Market

National Federation of Municipal Analysts

The National Federation of Municipal Analysts published a white paper in November 2020 calling for municipal bond issuers to "conduct a cybersecurity assessment to start the process of addressing cybersecurity risks as soon as possible" and recommending best practices for cybersecurity risk disclosures. Issuers and borrowers may want to review the paper to understand the views of municipal investors in this area.

Rating Agencies

While the SEC's proposed rules focus on enhancing and standardizing cybersecurity disclosure for public companies, rating agencies remain focused on public companies' cyber defenses and mitigation strategies when assessing the strength of a particular credit. A recent Moody's survey revealed that approximately 93% of organizations surveyed have a cybersecurity manager, and approximately 57% of North American organizations surveyed maintain cyber insurance.[3] To remain competitive, issuers and borrowers may want to consider implementing a cybersecurity manager, maintaining cyber insurance, and instituting cyber defenses and mitigation strategies to maintain their relative credit strength.

What's Next?

The SEC's proposed disclosure rules for public companies regarding cybersecurity incidents and related policies are not yet final. Orrick will continue to monitor the proposed rules and any related enforcement actions by the SEC, along with potential implications for issuers and borrowers in the municipal market.

---

[1] In *In re Pearson plc* (2021), the SEC imposed a penalty of $1,000,000 against Pearson plc because its risk factor disclosure implied only that the company faced a hypothetical risk of a data privacy incident and failed to disclose that the company had in fact already experienced such a data breach.

[2] In *In re First American Financial Corporation* (2021), the SEC imposed a penalty of $487,616 against First American Financial Corporation because, despite an employee's discovery of a security vulnerability, the company's reporting system was insufficient to ensure that the fact of the vulnerability was communicated to senior executives responsible for disclosure.

[3] *See* Cyber risk survey of issuers finds growing investments, but gaps in preparedness, Moody's Investors Service (March 31, 2022).

by Joseph Santiesteban, Sean Yates

May 17, 2022

Orrick, Herrington & Sutcliffe LLP