Bond Case Briefs

Municipal Finance Law Since 1971

Growing Cybersecurity Risks in the Municipal Bond Market: Frost Brown Todd LLP

In November 2024, the Township of White Lake, Michigan, fell victim to a cyberattack resulting in the wiring of approximately $29 million to the unauthorized account of the culprit. Before White Lake imminently closed on its issuance of general obligation bonds to finance new governmental buildings, the hacker was able to access the township's email system, impersonating an official of the township and sending altered wiring instructions to the underwriter of the bond. At the closing, instead of the township account, the purchase price was wired to the hacker. The sale of the bonds was ultimately canceled, and to this date, only approximately $21 million of the purchase price has been recovered. The underwriter is suing the township for the remainder.

Cyberattack Frequency and Disclosures

In recent years, there has been an increase in the frequency and media coverage of cyberattacks, from phishing scams to ransomware, and corporations are constantly working to stay ahead of bad actors by improving policy and technology. As evidenced by the White Lake cyberattack, the municipal markets are not immune to this threat—in fact, the public sector was the third most targeted sector by foreign nation-state cyber threat actors in 2024, according to Microsoft Threat Intelligence's global 2024 Digital Defense Report.

Tracking the rate of these incidents in the municipal market can be difficult, as there are currently no official guidelines from the Securities and Exchange Commission (SEC) pertaining to municipalities and their disclosure of cybersecurity risks or attacks. Issuers may be hesitant to make such disclosures for fear of the negative impact on their credit ratings and the associated negative publicity. This hesitation is well founded: two issuers, one in California and one in Maryland, recently had their credit downgraded after suffering cyberattacks. However, experts believe that, despite the potential credit impact, disclosure is essential, as it allows law enforcement to better understand cyberattack trends, build their databases, and develop strategies to prevent future attacks.

Continue reading.

Frost Brown Todd LLP – Ben Hadden and Chris Ansell

July 30, 2025