Bond Case Briefs

Municipal Finance Law Since 1971

Cyber Threats in Public Finance: Protecting Transactions from Wire Fraud - Orrick

A recent cyberattack on a Michigan township has exposed weaknesses in the bond-closing process. In this incident, hackers stole over $25 million in bond proceeds by using spoofed email addresses to provide fraudulent wire instructions.

The Michigan attack is not unique — Costs of Issuance have been stolen in connection with other transactions using similar techniques. As hacking becomes more sophisticated, the public finance industry must act now to add enhanced controls during the closing process, including, but not limited to:

- Providing all wire information solely to the Trustee or Paying Agent at least five business days in advance of closing;
- Requiring that the Trustee or Paying Agent confirm such wire information by telephone using the contact information provided on the Interested Parties list;
- Using encrypted email channels and documents to transmit wire information; and
- Requiring two separate confirmations from different people by telephone to a trusted counterparty before making any changes to already-provided wire information.

For more detailed recommendations on minimizing the risk of misdirected wire transactions or business email compromise fraud, please reach out to any of the authors: Aravind Swaminathan, Jenna Magan, Joseph Santiesteban, John Palmer, Sean Yates.

January.30.2025