Articles + Publications | March 11, 2025

Need for Enhanced Cybersecurity in Public Finance — Cyberthieves Steal Bond Proceeds

WRITTEN BY

Karen S. D. Grande | Walter J. St. Onge, III

Recent events highlight the need for enhanced cybersecurity protocols in government offices across the U.S. In late November 2024, the Township of White Lake in Michigan, intended to issue approximately $29 million in general obligation bonds to finance a new public safety building and a new township hall. Prior to closing, a criminal actor gained access to the township's email system, impersonated a township official, and altered emails containing wiring instructions. The bond underwriter, then wired the purchase price to the hacker rather than the township. The sale was canceled, and to date, approximately $23.6 million has been recovered and returned to the underwriter, which is suing the township for the remainder. According to a supplemental disclosure posted by the township on March 11, the U.S. Securities and Exchange Commission has opened an investigation regarding this event and the sale of the township's bonds to determine if any violations of the federal securities laws have occurred.

What can governmental entities transferring (and receiving) large sums of money do to better protect themselves from cybercriminals? Many have set up protocols and procedures with vendors and others with whom they frequently do business. Bond financings, however, are usually infrequent for most governmental units, and involve underwriters, financial advisors, paying agents, and other parties that government staff may not know well and with whom they may have little contact.

The Government Finance Officers Association (GFOA) recently recommended a series of fraud prevention measures for participants in public finance transactions to adopt. The recommendations, which may be found at Fraud Prevention Measures When Receiving Funds, include establishing protocols with all vendors and transaction participants regarding (i) how any banking information will be communicated, (ii) by whom, and (iii) in what manner, such as telephone or video meeting. The GFOA recommends the use of encrypted email for transmitting sensitive information and reiterates the importance of maintaining good cybersecurity practices, such as not relying on any information or link contained in an email, but rather contacting the purported sender via prior, known contact information. Another consideration is to require a purchaser, in advance of a closing date, to initiate a test wire in a de minimis, random amount, to the account of the issuer, followed up by telephone confirmation of the receipt and amount of such wire, thereby confirming the accuracy of the wire instructions.

White Lake's loss highlights the increasing risks to governmental units in transmitting and receiving funds, not only in public finance transactions but also in day-to-day business. Risks can be mitigated by appropriate staff training, close monitoring of financial transactions, implementation of robust protocols, and heightened vigilance by all transaction participants.

RELATED INDUSTRIES + PRACTICES

- Public Finance