Bond Case Briefs

Municipal Finance Law Since 1971

BE AWARE: Governments Being Hit by Sophisticated Electronic Fraud Scams.

All governments should be aware of recent electronic fraud and other sophisticated measures being used to access banking account and other payables information. These schemes include sending extremely realistic e-mails from fake or hacked e-mails disguised as known vendors, including banks. Governments should exercise caution in their handling of e-mails announcing changes to a vendor's ACH or other account information, or from vendors requesting the government's account information. GFOA is cautioning governments to be aware and put safeguards in place to prevent fraud.

At GFOA's annual conference last month in Denver, the *Addressing Fraud in Electronic Payments* session focused on this topic. Speakers provided their own tales of how their governments' accounts had been or were nearly breached by sophisticated fraud attempts. Slides from the presentation, which are available on the GFOA website, provide valuable information about establishing policies and procedures to prevent and react to this type of fraud, as well as details about how it is executed.

Some key elements to help governments avoid being the victim of fraud include the following recommendations:

- Do not make any changes to vendor information, particularly payment addresses and/or bank account information, without carefully reviewing the information provided and corroborating the change through other sources.
- **Do not use e-mail to confirm changes to vendor payment information**—if the government or vendor has been recently hacked, you will likely be contacting the fraudster rather than the vendor. Verify changes by phone or regular mail, using information from existing vendor records.
- Revise the government's forms to require that vendors provide both the old and new bank routing and account numbers or billing addresses when requesting a banking change or a payment mailing change.
- Remove vendor change forms from the government's website to help avoid this kind of scam. Instead, ask vendors to contact staff directly for these forms.
- Communicate with staff and outside departments about the importance of prioritizing outstanding balance inquiries from vendors and resolving them quickly. Payment questions need to be addressed as quickly as possible because they may uncover vendor or payment fraud. Again, insist that staff use telephones, faxes, or the postal service for correspondence rather than e-mail to address issues with vendors.

If you are aware of fraudulent account routing and numbers, notify your bank and law enforcement. They may already be involved in a related investigation and might be able to help.

Download the slides from the GFOA conference.