**Wayne A. Johnson**
State Auditor

**C. Jack Emmons,** CPA, CFE
Deputy State Auditor

**State of New Mexico**
**OFFICE OF THE STATE AUDITOR**

For Immediate Release
July 17, 2018

Contact: Enrique C Knell
505-551-2407

# State Auditor Wayne Johnson warns government entities about costly invoicing scam

*City of Alamogordo lost $250,000 to fake vendor*

**Santa Fe, NM** – The City of Alamogordo last week paid more than $250,000 to an unknown scam artist, and recovery of that public money is likely to be difficult if not impossible. In light of that scam, State Auditor Wayne Johnson is reminding all of the state's government entities to be extremely cautious and aware when it comes to e-mail communication from any vendors.

A staff member with the City of Alamogordo received an email request to change banking information from someone who appeared to be a representative of Cooperative Education Services, (CES) a New Mexico purchasing cooperative. The email appeared to come from a person known to work for CES, and contained an outdated version of the CES logo. The City accepted the change in banking information and paid all invoices, only to discover that the email was fraudulent. CES is a commonly used purchasing cooperative for New Mexico schools, and other government entities. City leaders immediately notified law enforcement, including the FBI.

"In this Snapchat and Instant Message world, it's critical to verify information with a real person, either in person or by phone," said Johnson. "An email seeking to alter banking information should always be a red flag. Talk to your vendors, especially when they do something out of the ordinary, like send a change in banking information. It's important to establish personal relationships so that finance staff can talk to people already known to them. There's no excuse for not taking that extra step to make sure to prevent the theft of a quarter of a million dollars in public money."

Alamogordo officials have acknowledged that the amount owed to the company was correct, so the request for payment was not unusual. The e-mail appeared to come from an agent the procurement officer knew and had worked with in the past. It bore an official looking logo from CES. The procurement officer didn't question or confirm the e-mail and the information contained within it. She forwarded it to the finance department which changed the payee information as requested. Payment for outstanding invoices was made for more than $250,000 and went to the fraudulent bank account instead of to the actual vendor.

Later, representatives from CES called requesting payment on the still outstanding invoices. Managers believed payment had already been made, and only then realized they had transferred money to a fraudulent entity.

Today CES is notifying all customers of the potential for fraud. CES has advised the OSA that it has not changed their banking information, nor do they plan to do so.

“Our office has warned local governments before about e-mail scams,” said Johnson. “Those who handle public dollars need to pay attention and realize these scams can happen at any time and they are constantly evolving. These thieves are creative and effective. Public entities have to make sure they have strong anti-fraud procedures and that they are following them in every instance in order to safeguard public money.”

Johnson’s office warned government entities late Friday via the following risk advisory: https://www.saonm.org/media/uploads/GAO-Risk_Advisory-250Kscam2018-07-13.pdf

—End—