Timothy M. Keller
State Auditor

Sanjay Bhakta, CPA, CGFM, CFE, CGMA
Deputy State Auditor

State of New Mexico
OFFICE OF THE STATE AUDITOR

To: **ALL AGENCIES AND IPAs**
From: **TIM KELLER, STATE AUDITOR**
Subject: **FRAUD PREVENTION ALERT**
Date: **APRIL 3, 2017**

The Office of the State Auditor (OSA) has received information that governmental agencies are being targeted by imposters through a vendor fraud scheme. In one recent instance, the scheme resulted in the loss of over $200,000 in public funds from a public school in New Mexico.

How Vendor Payment Scams Work

Specifically, the scam involves several steps. Imposters use publically available information to get the contact information (usually email) of the employee handling financial transactions for the agency. This may be done through a seemingly routine call to the agency or by gathering information from the agency's website. The imposters also identify an agency vendor through public or inside information. Next, the imposters send an email to the employee that appears to be from a known vendor (the email address is usually spoofed or is very similar to that of the company's). The email requests that the payment method for the vendor be changed, such as changing payments to direct deposit, sending the payment to a new address, or requesting that a wire transfer be sent to a different bank or account.

Steps to Prevent Losses

All agencies should evaluate their internal controls designed to prevent and detect vendor payment frauds as well as other types of schemes. Employees should receive routine training and management should monitor that appropriate controls are being adhered to.

These controls should include, but are not limited to directly verifying the legitimacy of any such request. Any changes to payment or banking information should be checked with the vendor and/or payee prior to processing. This should be done through a phone number or contact person obtained through a known source, such as their public website, not the person or number listed in the email. Additionally, please see the June 2016 OSA Risk Advisory (attached) regarding wire transfer schemes.

Upon learning of an attempted or successful scam, agencies should immediately notify their banking institution and report the matter to law enforcement. Any losses must also be reported to the OSA pursuant to NMSA 1978, Section 12-6-6.

2540 Camino Edward Ortiz, Suite A, Santa Fe, New Mexico 87507
Phone (505) 476-3800 * Fax (505) 827-3512
www.osanm.org * 1-866-OSA-FRAUD

GAO

Government Accountability Office

New Mexico Office of the State Auditor

Risk Advisory
Government Email Wire Transfer Scams

The Office of the State Auditor (OSA) has issued this Risk Advisory to alert governmental agencies in the State of New Mexico of a pattern of ongoing scams in which employees are asked to make wire transfers based solely on email communication. The OSA strongly advises management and governing bodies to ensure safeguards are in place to prevent and detect inappropriate wire transfer requests, and to establish a "tone at the top" that encourages employees to question payment requests that deviate from standard procedures.

Resources

FBI Internet Crime Complaint Center (IC3)
http://www.ic3.gov/complaint

New Mexico Department of Information Technology (DOIT)
www.doit.state.nm.us

Multi-state Information Sharing and Analysis Center
https://msisac.cisecurity.org/
U.S. Department of Homeland Security - www.dhs.gov/cyber

National Cyber Security Alliance - www.StaySafeOnline.org

The OSA has received notice of three recent attempted wire transfer schemes specifically targeting local governments in order to steal public money. While one county government and two school districts most recently reported to the OSA, the OSA is aware that other organizations have been observing a pattern of these schemes across the state. In all three incidents reported to the OSA, the administrative staff followed up with questions in outgoing emails and received responses that added to the legitimacy of the wire transfer requests. All three entities processed the wire transfers and subsequently became suspicious enough to contact banking authorities to attempt to reverse the transactions. Two of the three entities were able to prevent the loss of public money. The diagram on the following page uses redacted versions of real emails that government employees received to highlight the indicators of fraud.

Internal Controls

Adherence to established internal controls regardless of the situation is critical to safeguarding public funds. It is critical that staff are properly trained on internal control procedures and that the "tone from the top" allows staff to question deviations from policies and procedures.

The OSA has the following various recommendations that agencies may consider when assessing their internal controls of expenditures and disbursements:

- Requiring purchase requisitions, purchase orders and detailed invoices prior to making payments.
- Segregating duties among the creator of the purchase order, the good recipient and the payment approver.
- Requiring a full set of supporting documents before transactions with a new vendor.

Visit our website at: www.osanm.org/government_accountability_office.

GAO
Government Accountability Office
New Mexico Office of the State Auditor

In addition, specifically with respect to email scams, agencies should consider:

- Developing enterprise network and email controls based on industry best practices.
- Training staff to be alert for malicious or suspicious emails and to appropriately report their suspicions.
- Requiring periodic password changes for network and email accounts.
- Working with agency banking partners to take advantage of available banking controls, including those that restrict automated clearinghouse and wire transfers to only specifically listed accounts.

Red Flags in Email Scams

(Excerpts from real emails that government employees received)