



STATE OF INDIANA
AN EQUAL OPPORTUNITY EMPLOYER

STATE BOARD OF ACCOUNTS
302 WEST WASHINGTON STREET
ROOM E418
INDIANAPOLIS, INDIANA 46204-2769

Telephone: (317) 232-2513
Fax: (317) 232-4711
Web Site: www.in.gov/sboa

MEMORANDUM

TO: All Local Officials
FROM: Paul D. Joyce, CPA , State Examiner
RE: Recent Fraud Schemes
DATE: May 11, 2020

We wanted to alert you to a couple of situations that came to our attention recently. Even during a worldwide public health emergency, fraudsters and scammers are still working to try and get your money. Please be alert to the following areas:

FRAUDULENT CHECKS

We received information last week that a local governmental entity became a victim of fraud when their bank account information and bank routing number were compromised and used to create false and fraudulent checks. Fraudsters who create these false checks with governmental bank account information present them at banks across the country, thereby stealing public funds.

Sometimes a bank where false checks are presented will question their legitimacy and perhaps contact you to verify they were issued by you. But that does not always happen and funds from your accounts can be taken. Oftentimes, if unauthorized payments from a bank account are brought to the attention of the bank in a timely manner, the bank will replace the amount that was stolen. However, if you are not reviewing your bank activity frequently or reconciling monthly, you would not be aware of these fraudulent transactions and the delay in reporting them to the bank may make it more difficult to get the bank to restore the funds to the bank account.

Review bank account information frequently and your bank statement monthly and verify that all of your recorded deposits are credited to your account and all withdrawals from the account are transactions that trace to checks prepared by your office or electronic funds transfers that you have authorized. By doing this, you can identify any fraudulent activity on your account, as well as any potential bank errors, as early as possible.

We recommend you consider the use of positive pay files through your bank, which is where a bank compares checks presented for payment with a list of checks the governmental unit has authorized. If a check is presented that isn't authorized, like the fraudulent checks described above, the bank will not honor it and your funds remain protected. If you do not employ the use of positive pay files through your bank, it is especially important that you monitor your bank activity as often as possible. But do work with your bank. They may have other ideas on fraud detection and prevention that could be tailored to your unit, such as the unit utilizing a confirmation system with the bank prior to the bank's payment of any check over a certain dollar amount.


RANSOMWARE

A local governmental entity recently became a victim to ransomware. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. The principle of ransomware is that the malware encrypts files on a system's hard drive using an unbreakable key, and this is decrypted by the attacker once a ransom is paid. Beware of unexpected or suspicious emails, especially those containing a link or requesting a reply. Most ransomware is delivered via email and the typical overall themes are shipping notices from delivery companies. Also, many attacks are delivered by mass random emails because the intention is to infect as many as possible to maximize the chances of getting a result.

Consider your unit's policies related to the protection of computer information. The most common advice to recover from an attack by ransomware relies largely on whether a good backup policy is employed. Backup expectations are discussed in the various *Accounting and Uniform Compliance Guidelines Manuals* for the various types of political subdivisions, which are available on our website (<http://in.gov/sboa/index.htm>). Governmental entities also should keep their anti-virus software up-to-date and apply security patches in a timely manner.

Should you become the victim of either of these schemes, contact the appropriate law enforcement authorities, the Indiana State Board of Accounts, and your computer software vendor. When contacting the Indiana State Board of Accounts, please call or email the Directors of Audit Services for your particular governmental unit type and/or the Director of Special Investigations. All may be reached by phone at 317-232-2512 or 317-232-2513. Email contacts are:

Special Investigations	mmahon@sboa.in.gov
Counties	counties@sboa.in.gov
Cities & Towns	cities.towns@sboa.in.gov
Schools	schools.townships@sboa.in.gov
Libraries	libraries@sboa.in.gov
Townships	schools.townships@sboa.in.gov
Special Districts	specialdistricts@sboa.in.gov


Paul D. Joyce, CPA
State Examiner