



Office of the Washington State Auditor
Pat McCarthy

Fraud Investigation Report

City of Tenino

For the investigation period January 1, 2020, through June 30, 2020

Published January 13, 2022

Report No. 1029267



Find out what's new at SAO
by scanning this code with
your smartphone's camera



**Office of the Washington State Auditor
Pat McCarthy**

January 13, 2022

Mayor and City Council
City of Tenino
Tenino, Washington

Report on Fraud Investigation

Attached is the official report on a misappropriation at the City of Tenino. On May 5, 2021, the City notified the Office of the Washington State Auditor of a potential loss of public funds. This notification was submitted to us under the provisions of state law (RCW 43.09.185).

Our investigation was performed under the authority of state law (RCW 43.09.260) and included procedures we considered necessary under the circumstances.

If you are a member of the media and have questions about this report, please contact Director of Communications Kathleen Cooper at (564) 999-0800. Otherwise, please contact Special Investigations Program Manager Stephanie Sullivan at (360) 688-0858.

Pat McCarthy, State Auditor
Olympia, WA

cc: Kayleen Canup, Clerk-Treasurer

Americans with Disabilities

In accordance with the Americans with Disabilities Act, we will make this document available in alternative formats. For more information, please contact our Office at (564) 999-0950, TDD Relay at (800) 833-6388, or email our webmaster at webmaster@sao.wa.gov.

FRAUD INVESTIGATION REPORT

Background and Investigation Results

On May 5, 2020, the City of Tenino notified our Office regarding a potential loss of public funds, as state law (RCW 43.09.185) requires. The City has 13 employees and an annual operating budget of just more than \$1 million.

On March 19, 2020, a phishing email was sent to multiple public employees in Washington State, including the City of Tenino's Clerk-Treasurer. All of the recipients were members of the same nonprofit professional association. The email was designed to look like it came from the past president of the association and asked recipients to help the organization pay some of its bills, which is not a normal business practice.

On the same day the phishing email was sent, the association sent an email to all of its members, including the Clerk-Treasurer, notifying them that the request was illegitimate. The association also asked its members not to make any payments and report the phishing email to their IT departments. While other recipients either deleted or ignored the email, contacted the association to confirm it was a phishing attempt, or contacted their IT departments, Tenino's Clerk-Treasurer did not. Instead, on the same day as receiving the email, he initiated an automated clearing house (ACH) payment for \$2,890 to someone in Ohio who was not connected to either the City or the association.

Tenino's Clerk-Treasurer was the only recipient of the phishing email who made payments. Based on additional emails claiming to be from the association, the Clerk-Treasurer continued to initiate ACH payments until May 5, 2020. These emails listed multiple out-of-state people and banking information for the payments.

On May 5, 2020, the Clerk-Treasurer said a Texas-based bank called to report a concern about one of the ACH payments. The bank said someone came in to withdraw funds that the City had recently deposited and attempted to close the account. The Clerk-Treasurer asked the bank to contact the professional association about the payment, and then he contacted the Mayor to say he had been deceived into a scam for City funds. When the bank contacted the professional association's president that same day, she knew nothing about the payments. On the same day, the Clerk-Treasurer reported the loss to our Office and the City of Tenino police. The Tenino police contacted the Washington State Patrol (WSP), who conducted an investigation.

We reviewed WSP's investigation and agree with its conclusions. Additionally, we calculated \$336,968 in inappropriate ACH payments. Of this amount, \$56,659 has been credited back to the City, resulting in an overall loss of \$280,309 between March 20, 2020, and May 4, 2020. WSP closed its case and referred it to the Federal Bureau of Investigation (FBI).

WSP's investigation found the following:

- The Clerk-Treasurer served in the U.S. military until 2016 and received specialized training in cybercrimes. He joined the City of Tenino in May 2016 as the Clerk-Treasurer.
- During an interview with WSP, the Clerk-Treasurer said he recognized that the emails did not come from the association's official email address. Despite that, he said he did not call the professional association to confirm the legitimacy of the payment request because he recognized the name of the person who claimed to send the email. The Clerk-Treasurer said he asked the City Council for its approval before making payments, but acknowledged that he did not get the council's approval for every payment. He said that he never received invoices or supporting information for the payments, but he didn't care as long as the association reimbursed the City for the transactions. He said he convinced himself that he was communicating with the real professional association's president, and that he did not realize he had been deceived until the out-of-state bank called him.
- Between March 19, 2020, and May 4, 2020, the Clerk-Treasurer initiated 20 ACH payments from the City's bank account. These payments went to multiple out-of-state bank accounts. WSP obtained search warrants for bank account records associated with the ACH payments. WSP's review of these records found that multiple accounts were opened and then quickly closed after the City's funds were deposited and withdrawn.
- During the time of these payments, the Clerk-Treasurer informed the City Council at the end of a regular meeting that he had received a request from a professional association asking for help paying its expenses for its annual conference rescheduling. During this meeting on April 14, 2020, the Clerk-Treasurer asked for Council for its approval to "write a couple of checks" to help the organization. He said the association temporarily lacked the ability to write checks because its treasurer was out of the office due to COVID-19. None of this information was true, and none of the phishing emails went into that level of detail. Ultimately, the Council approved \$23,000 for this purpose, and the Clerk-Treasurer said the City would be reimbursed in about two weeks. He did not disclose that he already had paid \$45,090 to purportedly help the association.
- In July 2020, WSP obtained a search warrant for the account information related to the phishing email and found that it originated from the country of Nigeria. WSP's investigation noted other red flags about the email that someone knowledgeable in cybersecurity should notice, including spelling and grammatical errors, that it did not come from an email address connected to the association, that the sender was not the association's current president, and the frequency and use of multiple out-of-state bank accounts.
- WSP could not continue to investigate once the funds were withdrawn and the accounts were closed because that activity happened in other states.

In December 2020, the Clerk-Treasurer resigned from his position and moved out of state. In January 2021, WSP closed its investigation, concluding that it could not determine whether the

Clerk-Treasurer personally benefitted from the City's loss. WSP turned over its files to the FBI for further investigation.

Control Weaknesses

The City's internal controls were inadequate for safeguarding public resources. We found the following weaknesses allowed the loss to happen:

- The Clerk-Treasurer had full access to all of the City's bank accounts, and he had the ability to complete electronic transfers with no oversight or monitoring.
- The Clerk-Treasurer also performed bank statement reconciliations without someone else reviewing them.

Recommendations

We recommend the City improve its internal controls over disbursements and banking. At a minimum, the City should implement a secondary bank statement reconciliation that includes a review of supporting details related to ACH disbursements. We further recommend the City work with its bank to determine appropriate ACH and wire disbursement authority and dollar thresholds.

Additionally, the City should reassess its overall control structure. The City should evaluate which key duties can and should be segregated among staff. Where segregation of duties is not possible, City should consequently increase monitoring.

City's Response

The City of Tenino has taken extreme measures to improve the internal controls and monitoring over disbursements and banking to prevent future fraudulent activities.

The control measures the City has implemented to safeguard public resources are as follows:

The City's ACH transaction process is now secured with dual control. With dual control, one employee initiates the ACH batch process, the banking system sends an email to the two other authorized employees, one of the employees who receives an email will have to log into the banking system by using their own personal credentials and can then approve the ACH batch. The employee who initiates the ACH transaction cannot approve it. This process is limited to three people. There is a set dollar limit for ACH transactions.

The City's wire transfer process is set up in a similar way as ACH transactions. Wire transfer transactions can be initiated through online banking. Once initiated, the bank will call one of four people to authorize the transaction. Everyone on the call list has their own password that the bank will request in order to approve the transaction. The bank only requires approval from one individual, excluding the person that is initiating the transaction. There is a set dollar limit for wire transfer transactions.

When doing bank reconciliations, the Clerk/Treasurer will reconcile the receipts and disbursements by matching all transactions on the bank statements to all transactions that have been entered into the City's financial software program. Once completed, these documents will be presented to the Mayor who will then review them as well.

The City has contracted with an IT company, Right! Systems, Inc., who have been instrumental in the process of security hardening for the protection of IT resources. Right! Systems, Inc. has set up a Multi-Factor Authentication (MFA) that will require an additional step in the accessing of the City's network. When an employee attempts to login, a message will be sent to a cell phone or key fob for approval by that individual. Right! Systems, Inc., is implementing email monitoring and filtering. This monitoring and filtering will analyze all email traffic prior to sending to protect against phishing and will analyze links sent in email prior to allowing an employee to visit sites outside the network. Right! Systems, Inc., will also monitor the use and updating of the firewall, anti-virus protection, anti-malware protection and anti-spam protection.

The City of Tenino will continue to be diligent by improving and strengthening the internal controls and monitoring of funds through all available resources to prevent any fraudulent activities in the future.

Auditor's Remarks

We thank City officials and personnel for their assistance and cooperation during the investigation. We will follow up on the City's internal controls during the next audit.

ABOUT THE STATE AUDITOR'S OFFICE

The State Auditor's Office is established in the Washington State Constitution and is part of the executive branch of state government. The State Auditor is elected by the people of Washington and serves four-year terms.

We work with state agencies, local governments and the public to achieve our vision of increasing trust in government by helping governments work better and deliver higher value.

In fulfilling our mission to provide citizens with independent and transparent examinations of how state and local governments use public funds, we hold ourselves to those same standards by continually improving our audit quality and operational efficiency, and by developing highly engaged and committed employees.

As an agency, the State Auditor's Office has the independence necessary to objectively perform audits, attestation engagements and investigations. Our work is designed to comply with professional standards as well as to satisfy the requirements of federal, state and local laws. The Office also has an extensive quality control program and undergoes regular external peer review to ensure our work meets the highest possible standards of accuracy, objectivity and clarity.

Our audits look at financial information and compliance with federal, state and local laws for all local governments, including schools, and all state agencies, including institutions of higher education. In addition, we conduct performance audits and cybersecurity audits of state agencies and local governments, as well as state whistleblower, fraud and citizen hotline investigations.

The results of our work are available to everyone through the more than 2,000 reports we publish each year on our website, www.sao.wa.gov. Additionally, we share regular news and other information via an email subscription service and social media channels.

We take our role as partners in accountability seriously. The Office provides training and technical assistance to governments both directly and through partnerships with other governmental support organizations.

Stay connected at sao.wa.gov

- [Find your audit team](#)
- [Request public records](#)
- Search BARS manuals ([GAAP](#) and [cash](#)), and find [reporting templates](#)
- Learn about our [training workshops](#) and [on-demand videos](#)
- Discover [which governments serve you](#) — enter an address on our map
- Explore public financial data with the [Financial Intelligence Tool](#)

Other ways to stay in touch

- Main telephone:
(564) 999-0950
- Toll-free Citizen Hotline:
(866) 902-3900
- Email:
webmaster@sao.wa.gov