Office of the Washington State Auditor
Pat McCarthy

Fraud Investigation Report

Washington Counties Insurance Fund

For the investigation period December 12, 2023 through September 30, 2024

Published April 7, 2025

Report No. 1036934

Scan to see another great way we're helping advance #GoodGovernment

Office of the Washington State Auditor
Pat McCarthy

April 7, 2025

Board of Trustees
Washington Counties Insurance Fund
Tumwater, Washington

Report on Fraud Investigation

Attached is the official report on a misappropriation at the Washington Counties Insurance Fund. On October 7, 2024, the Fund 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).

This report contains the results of our investigation of the former Finance Manager's unallowable activities at the Fund from January 11, 2024 through September 23, 2024. The purpose of our investigation was to determine if a misappropriation had occurred.

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: Bobby Jackson, Executive Director and Amber Haslett-Kern, Finance Manager

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

Investigation Summary

On October 7, 2024, the Fund notified our Office regarding a potential loss of public funds, as required by state law (RCW 43.09.185). On September 18, 2024, the Fund terminated its Finance Manager. Fund staff subsequently identified several electronic payments on its bank statements that were not recorded in the accounting system. Further review found additional electronic payments paid to the Finance Manager after he was terminated.

We investigated and determined the Finance Manager misappropriated $123,404 in electronic disbursements and excessive payroll payments, and a credit card charge of $273 between January 11, 2024, and September 23, 2024.

The Fund experienced an earlier loss of public funds in 2024. On February 8, the fund reported that the Finance Manager received multiple phishing emails requesting he process electronic payment invoices totaling $54,898, which he paid and did not record in the accounting system.

Based on the information available at the time of reporting to our Office, this loss did not appear to indicate potential employee involvement. Given the substantiated payroll misappropriation by the Finance Manager, however, we later reexamined the cyber losses. This review was inconclusive if the Finance Manager personally benefited from them.

The Fund filed a report with the City of Tumwater Police Department, which is investigating this case. We will refer this case to the Thurston County Prosecuting Attorney's Office.

Background and Investigation Results

The Fund, located in Thurston County, operates on an annual budget of about $2.12 million, including approximately $709,000 in payroll expenses. The Fund pools the cost of employee benefits such as medical, dental, vision and life insurance coverage for counties and special purpose districts throughout the state. A 21-member Board of Trustees governs the Fund. Daily operations of the Fund are run by an Executive Director and six other employees. The Finance Manager maintains key financial system access and is responsible for the oversight of all financial records including recording payments in the accounting system, reconciling accounting system records to banking records, processing electronic vendor payments and payroll. These responsibilities require the Finance Manager to maintain online banking access to Fund bank accounts.

In December 2023, the Fund contracted with a temporary hiring agency for a full-time bookkeeper to help with various financial activities. Beginning January 1, 2024, the Fund formally hired the temporary bookkeeper as its new Finance Manager. On January 3, 2024, the Finance Manager created and processed payroll mid-month draws to himself and other employees much earlier than expected. On January 4, 2024, the Finance Manager received a phishing email designed to appear

as if the Executive Director was requesting the Finance Manager process an electronic payment for an unpaid invoice totaling $2,434. The Finance Manager paid the invoice, and it was disbursed the next day from the Fund's bank account.

On January 11, 2024, the Finance Manager processed a second unauthorized mid-month payroll draw for himself.

Further, from January 8, 2024, to January 30, 2024, in response to additional phishing emails for unpaid invoices, the Finance Manager created and processed seven additional electronic payments totaling $52,465. The Finance Manager did not discuss the legitimacy of the emails with the Executive Director until February 8, 2024, when the Executive Director said he had not sent any of the emails. The Executive Director reported the loss of public funds to our Office the same day. Based on the information available at the time of reporting to our Office, this loss did not appear to indicate potential employee involvement.

On September 16, 2024, the Finance Manager left his work issued cell phone and computer at the Fund's office. On September 18th, 2024, due to work performance issues, the Fund terminated the Finance Manager. That same day, the Fund contacted the bank to remove the Finance Manager's online banking access, however, the bank did not remove access until several days later.

Over the next several weeks, while reconciling accounting system records to banking records, staff identified several electronic payments on bank statements that were not recorded in the Fund accounting system. On October 6, 2024, the bank provided receipting records that showed these were payments to the Finance Manager that exceeded his normal monthly paychecks. Additionally, the Finance Manager made unauthorized electronic payments to himself after he was terminated.

On October 7, 2024, the Fund reported the additional loss of public funds to our Office and we opened an investigation.

Our investigation focused on the Fund's bank account activity and the financial areas the Finance Manager had access to, such as electronic payments, payroll, and credit cards. Our review found:

- The Finance Manager processed 27 unauthorized electronic payments, and one payroll draw between January 11, 2024, and September 12, 2024, and then three additional unauthorized electronic payments after his employment with the Fund ended.
- Combined, these disbursements and payroll payments totaled $123,404 in misappropriation. The Finance Manager created and processed all payments to his personal bank account, and did not record any in the Fund's accounting system, thereby further concealing the misappropriation.
- The Finance Manager made a personal charge on July 29, 2024, for $273 related to food, clothing and a personal printer.

We re-examined the earlier cyber loss to determine if the Finance Manager may have personally benefited. On November 15, 2024, we obtained a court order for the Finance Manager's personal bank account records and the bank account records related to the reported February 8, 2024, loss.

Our review of the Finance Manager's personal bank records confirmed there were no additional misappropriated Fund amounts deposited into his account beyond those we had already identified. We observed that after misappropriated funds were deposited into his bank account, they were immediately withdrawn in cash or moved to a cash app account or cash card.

Our review of the bank account records related to the reported cyber loss, to determine if the Finance Manager personally benefitted from these payments, was inconclusive. Our review found:

- The Finance Manager created and processed eight electronic payments to the same vendor name and bank account, totaling $54,898 in loss between January 5 and January 30, 2024. The Finance Manager said he thought these payments were for legitimate invoices; however, a review of the Fund's accounting records showed he did not record any of the payments in the accounting system.
- When we compared bank account information for this reported cyber loss to the Finance Manager's personal banking information, we found the cyber loss payments and confirmed misappropriated payments went to different bank account numbers at the same bank. Bank records did not show the Finance Manager's name on the account into which the cyber loss funds were deposited.
- We observed that after the cyber loss funds were deposited into this account, they were immediately withdrawn into cash. We were unable to determine what became of the cash once withdrawn.
- The source for $11,063 in cash deposits to the Finance Manager's personal bank account in January 2024 could not be determined.

In October 2024, the City of Tumwater Police Department attempted to interview the former Finance Manager, who first asked if they were contacting him about the cyber loss reported on February 8, 2024. The Police Department asked about the electronic payments into his personal bank account beyond his normal payroll and he declined to answer any questions.

In February 2025 and March 2025, we attempted to contact the former Finance Manager for an interview. On March 20, 2025, we received a response from his attorney saying the former Finance Manager would not be available to speak with us directly for a significant amount of time.

Control Weaknesses

Internal controls at the Fund were not adequate to safeguard public resources. We found the following weaknesses allowed the misappropriation to occur. The Finance Manager:

- Had full access to the Fund's bank account and the ability to complete electronic disbursements, including for payroll, with limited oversight or monitoring.
- Was responsible for recording disbursments in the accounting system and performing bank statement reconciliations without a secondary, independent review.

Recommendations

We recommend the Fund evaluate and improve its internal controls over disbursements and banking. At a minimum, the Fund should implement a secondary bank statement reconciliation that includes a review of supporting details related to all types of electronic disbursements.

We also recommend the Fund seek recovery of the misappropriated $123,677 and related investigation costs of $15,323 from the former Finance Manager and/or its insurance bonding company, as appropriate. Any compromise or settlement of this claim by the Fund must be approved in writing by the Attorney General and State Auditor as directed by state law (RCW 43.09.260). Assistant Attorney General Matt Kernutt is the contact person for the Attorney General's Office and can be reached at (360) 586-0740 or Matthew.Kernutt@atg.wa.gov. The contact for the Office of the Washington State Auditor is Brandi Pritchard, Assistant Director of Special Investigations, who can be reached at (509) 726-1886 or Brandi.Pritchard@sao.wa.gov.

Fund's Response

We acknowledge receipt of the state auditor's report dated April 7, 2025, which details the findings from the recent investigation of the Washington Counties Insurance Fund. We appreciate the diligence and professionalism demonstrated by the audit team throughout this process.

After thoroughly reviewing the report, we confirm our understanding of the findings, and the recommendations outlined. Below is a summary of the key issues addressed, and the corresponding resolutions implemented:

1. *Control Weakness 1*

   Findings: The former Finance Manager had full access to the Fund's bank account and the ability to complete electronic disbursements, including for payroll, with limited oversight or monitoring

   Resolution: The Fund has evaluated and improved our internal controls with approvals from the Executive Director before any disbursements are made. The finances are reviewed by the Finance Manager and Executive Director on a regular basis. At present, this includes a quarterly review with the Financial Oversight Committee, and the Board is looking to establish a full Finance Committee with regular reviews by the end of the year.

2. *Control Weakness 2*

   Findings: The former Finance Manager was responsible for recording disbursements in the accounting system and performing bank statement reconciliations without a secondary, independent review

   Resolution: At present, the Finance Manager and Executive Director review each monthly bank statement before they are approved. With the addition of a Finance Committee, our goal is to have a board member with a financial background to provide a secondary review on a regular basis. As we are a small staff and do not have the ability or experience to provide a secondary reconciliation at this time, we will utilize the review process until we are able to hire an assistant to the Finance Manager in the near future.

3. *Recommendation to Recover of Misappropriated Funds*

   The Fund is currently working to file a claim against Umpqua Bank for the portion of misappropriated funds taken after the Finance Manger was dismissed, with the remaining funds and investigation costs, as well as the costs associated with having our former Finance Director onsite to assist in the reconciliation of all bank accounts to be claimed against the Fund's Crime Policy, or, at minimum, restitution provided by the courts. We have until June 30, 2025 to file the claim with our insurance carrier.

We have taken the necessary steps to ensure compliance and have established measures to prevent future occurrences of similar issues. Additionally, we are committed to ongoing monitoring and internal reviews to uphold transparency and accountability within our operations.

We appreciate the guidance provided through this audit and remain dedicated to maintaining the highest standards of governance and financial integrity. Please do not hesitate to contact us should you require further information or clarification on any of the corrective measures undertaken.

Auditor's Remarks

We thank Fund officials and personnel for their assistance and cooperation during the investigation. We will follow up on the Fund'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