Office of the Washington State Auditor
Pat McCarthy

Fraud Investigation Report

King County Rural Library District

For the investigation period September 29, 2021 through July 3, 2024

Published April 10, 2025

Report No. 1037001

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

Office of the Washington State Auditor
Pat McCarthy

April 10, 2025

Board of Trustees
King County Rural Library District
Issaquah, Washington

Report on Fraud Investigation

Attached is the official report on a misappropriation at the King County Rural Library District. On June 9, 2023, September 1, 2023, and August 13, 2024, the District notified the Office of the Washington State Auditor of potential losses of public resources. The District submitted these notifications to us under the provisions of state law (RCW 43.09.185).

This report contains the results of our investigation of the former Client Technology Services Systems Administrator's unallowable activities at the District from September 29, 2021, through March 23, 2023. Additionally, this report contains the results of our investigation of two additional similar losses at the District from June 6, 2023, through July 3, 2024. The purpose of our investigations 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 Adam Wilson at (564) 999-0799. Otherwise, please contact Special Investigations Program Manager Stephanie Sullivan at (360) 688-0858.

Pat McCarthy, State Auditor

Olympia, WA

cc: Erhiza Rivera, Finance &Facilities Controller

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 June 9, 2023, the District notified our Office regarding a loss of public funds, as required by state law (RCW 43.09.185). In March 2023, the District discovered five network switches it received on March 15 at the Service Center were missing from its inventory.

The District initiated an investigation that found multiple network switches and routers totaling $78,584 were misappropriated between September 29, 2021, and March 23, 2023. Of this amount, the former Client Technology Services Systems Administrator was responsible for misappropriating at least $14,169 of the assets.

Further, on September 1, 2023, and August 13, 2024, the District notified our Office regarding new losses of the same type of network switches. The District initiated new investigations for these instances, which found a total misappropriation of $66,123 and property damage losses of $1,400 occurred between June 6, 2023, and July 3, 2024. The District was unable to identify the person responsible for these losses and could not rule out former or current employee involvement.

We reviewed the District's investigations and agree with its conclusions. The District filed three reports with the Issaquah Police Department. We will refer all cases to the King County Prosecuting Attorney's Office.

Background and Investigation Results

The King County Rural Library District is one of the largest circulating libraries in the United States, with 50 community libraries and 17 outreach vehicles. A seven-member Board of Trustees, appointed by the King County Council, governs the District and its approximately 1,000 employees. In 2023, the budget for total general fund expenditures was $140.7 million. The Finance and Facilities and Technology Capital Investment Program received about $6.5 million to cover anticipated major expenditures for ongoing maintenance and upkeep of the District's capital assets. Between 2021 and August 2024, the District purchased 221 network switches and router equipment, totaling $453,825.06.

The District employs Client Technology Services Systems Administrators to manage computer hardware, software and related systems throughout the organization. The Systems Administrator is responsible for the day-to-day operations, evaluating system performance, and identifying and resolving concerns. The Systems Administrator is part of the Information Technology Services team.

After the District discovered five network switches were missing in March 2023, it opened an investigation and found that an additional 24 network switches and four network routers it received between September 29, 2021, and March 15, 2023, were also missing. The total cost of the 33 missing switches and routers was $78,584.

The District reviewed building access control records and security camera footage for the location and period of the initial loss and determined the former Systems Administrator was responsible for the misappropriation of at least five network switches, costing $14,169. Security camera footage and building access control records showed the former Systems Administrator entered the Service Center, and within the Service Center, the Information Technology Services Department, using an authorized electronic key card on March 20, 2023, in the area where the network switches and routers were stored, during an unexpected time of the day. While portions of the District's Service Center not comprising the Information Technology Services Department are not locked during normal business hours (i.e. front entry and public-access lobby) the entirety of the Information Technology Services Department is always locked, and access is only granted to employees.

The District's investigation into the other 24 missing network switches and four routers, including review of building access control records and security camera footage, ultimately lacked sufficient evidence to assign responsibility for those losses.

However, on March 27, 2023, the District interviewed the former Systems Administrator, who said he did not take the equipment. After the interview, the former Systems Administrator contacted the District through his union representative to facilitate his resignation as of April 14. He agreed to repay the District $66,000 for the missing network switches and routers. The $66,000 was based on the District's initial estimate of the total loss at the time they interviewed the former Systems Administrator. The District entered into an agreement requiring the former Systems Administrator to pay monthly installments of $916.44. As of January 2025, the former Systems Administrator has repaid $18,328.80.

Between June 6, 2023, and July 3, 2024, the District experienced three additional losses of 15 total network switches from the Information Technology Services Department within the Service Center building. The District again filed police reports and opened an investigation, which determined $66,123 in misappropriation of network switches and $1,400 in property damage losses occurred between June 6, 2023, and July 3, 2024. The District was unable to identify the person responsible for the losses and could not rule out former or current employee involvement.

We reviewed the District's additional investigation, which found the following:

- On June 7, 2023, Information Technology Services staff discovered five network switches costing $18,402 were missing from an order they unpacked the day before. In this instance of misappropriation, an unidentifiable person entered the secure area where the network switches were stored within the Information Technology Services Department. A universal key may have been used to bypass the electronic lock system. The District's building access control system recorded when the interior and exterior doors were accessed with no individual identification. The District subsequently rekeyed the physical locks to the Information Services Department, limited staff access to badge entry to track identifiable entry access information, and reduced authorized users of universal keys. They also added three security cameras to monitor all department entrances and exits to the area where switches were securely stored.

- On July 12, 2023, staff discovered that another four network switches, costing $14,721, were missing from a recently received order that had been stored within the secure Information Technology Services Department. In this instance, an unidentifiable person attempted to disable the security camera by unplugging the power source. The individual was seen on camera; however, their identity was concealed by wearing a hood and mask. After gaining access to the Service Center, possibly via a universal key to bypass the electronic lock system, they forcibly entered the secure Information Technology Services Department through the Director's office door to gain access to the Department and equipment, causing $1,400 in damages. The District's building access control system recorded when an exterior door was accessed with no additional identification. The District subsequently relocated switches to a temporary undisclosed secure location, installed additional surveillance cameras, rekeyed physical exterior locks to the Service Center, limited staff access to badge entry to track identifiable entry access information, further reduced authorized users of universal keys and repaired the Department door.
- On July 3, 2024, staff discovered another six network switches costing $33,000 were missing from an order purchased in 2023. In this instance, the network switches were stored in the Department awaiting configuration before they would have been dispatched to assigned locations. On the same day, an unidentifiable person is observed on camera forcibly entering the secure area of the Information Technology Services Department through the Department's interior side entrance to gain access to the equipment. It is unknown how they gained access to the Service Center. No record was logged in the building access control system to show entry to the building nor were damages to the exterior doors discovered. The District subsequently installed additional cameras throughout the interior and exterior of the entire building, and relocated switches to an alternative secured location.
- In all instances, the District reviewed security camera footage and building access control records but could not identify the person responsible for the misappropriation.

Control Weaknesses

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

- A universal key was likely used to enter the Service Center building for two incidents. When universal keys are used, the entry access logs for universal keys only show entry times but not identification of the keyholders.
- The District stored the newly purchased switches and routers in an open area of the Information Technology Service space before sending the network switches and routers to different library locations. Although there were security cameras installed, the cameras' line of sight did not cover the area where the equipment was stored.
- The District did not periodically conduct independent inventory checks of information technology (IT) equipment.

Recommendations

We recommend the District:

- Ensure it only distributes universal keys to authorized employees. Additionally, we recommend the District keep records of the keyholder's name and location of access.
- Store devices such as network switches and routers in a secure area within sight of security cameras
- Periodically conduct independent inventory checks to ensure all IT equipment is correctly tracked

The District entered into a restitution agreement with the former Administrator without seeking proper approval from the Attorney General and State Auditor as required by RCW 43.09.260. We recommend the District improve its fraud response plans to ensure it complies with this requirement for any potential future losses.

We also recommend the District seek recovery of related investigation costs of $9,758 from the former Administrator and/or its insurance bonding company, as appropriate. Any compromise or settlement of this claim by the District 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.

District's Response

The District is committed to safeguarding public resources and has a long-standing history of not experiencing any theft over several decades, prior the occurrence of the thefts described in this report. The District refutes any suggestion or assertion that internal controls to safeguard public resources were not being exercised by the District. Rather, we attest that the District had various internal controls described in this report in practice, to prevent and detect thefts from occurring. However, the intentional breach of authority granted and forced entries circumvented such controls.

The District took further measures to optimize its prevention and response upon the occurrence of each incident by reporting to its local Police Department, SAO, conducting internal investigations with outside legal counsel, enhancing the amount and quality of surveillance, and making changes to entry points and employee access as further described below. Below the District addresses each of SAO's recommendations in this report:

- *Ensure it only distributes universal keys to authorized employees. Additionally, we recommend the District keep records of the keyholder's name and location of access.*

SAO's investigation results asserts that a universal key was used to gain access, but this could not be determined. We would also like to note that the District has an established Key Control Policy with guidelines that include limiting employees authorized for access. The District monitors and tracks records of information of employee name, key, and description of access. These controls assisted the District in promptly conducting its internal investigations that resulted in the recovery of $66,000.

- *Store devices such as network switches and routers in a secure area within sight of security cameras.*

All Network switches and routers were stored within the secured-access-only Information Technology Services Department. After the first incident of theft, the security camera line of sight was modified, and multiple additional security cameras were installed to capture greater area of surveillance. External building surveillance cameras were also installed in multiple locations with enhanced optics.

- *Periodically conduct independent inventory checks to ensure all IT equipment is correctly tracked.*

The District routinely performs periodic internal audits of information technology equipment by the Finance department, throughout the 50 community libraries, Service Center, and Preston site and makes recommendation to enhance safeguards based on risks. As a result of the recent losses, IT has shifted the location of network switches and the Finance department has required these assets be tagged upon receipt for tracking in the asset inventory system. The District is also subject to Accountability Audits performed by SAO that may periodically involve testing of IT asset inventory.

We want to thank the State Auditor's Office for their efforts into the investigation.

The District will continue to work in partnership with the Attorney General and State Auditor and will seek approval as may be required by RCW 43.09.260 to the extent there are future losses.

Auditor's Remarks

State law (RCW 43.09.260(7)) requires the District to get written approval and consent of the Attorney General and the State Auditor for any settlement or compromise of any claim arising out of malfeasance. We reaffirm our conclusion and thank District officials and personnel for their assistance during the investigation. We will follow up on the District'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