Office of the Washington State Auditor
Pat McCarthy

October 20, 2025

Mayor and City Council
City of Lynnwood
Lynnwood, Washington

Management Letter

This letter includes a summary of specific matters that we identified during our accountability audit for January 1, 2024 through December 31, 2024.

These matters are not included as findings in our public report, but we view them as important enough to warrant the attention of management and the governing body. This letter will be referenced in our report.

This letter is intended for the information and use of management and the governing body as recommendations to help strengthen the City's internal controls. This letter is not suitable for any other purpose since it was not prepared for general distribution. However, this letter is a matter of public record and its distribution is not limited.

Thank you for being a partner in government accountability. We look forward to reviewing the status of these matters during your next audit.

Sincerely,

Haji Adams, Audit Manager

Insurance Building, P.O. Box 40021 • Olympia, Washington 98504-0021 • (564) 999-0950 • Pat.McCarthy@sao.wa.gov

Management Letter

City of Lynnwood
January 1, 2024 through December 31, 2024

Electronic payments

Since 2016, Washington's governments have reported more than $37 million of lost public funds as a result of cyberfraud, sometimes referred to as phishing, spearfishing or business email compromise schemes. In these schemes, an external threat actor contacts the government, appearing to be a known source such as an employee, upper-level manager, vendor or other business associate. Government staff are convinced to redirect valid payments to the external threat actor, or to purchase gift cards and provide them with the card numbers.

It is imperative that governments implement robust internal controls over all disbursements. This includes establishing a verification process for all requests to change an employee's or vendor's contact and payment information, as well as any requests to purchase gift cards, especially when they come through email, phone, fax or another electronic method.

The City spent about $41.8 million in payroll in fiscal year 2024. The City is responsible for establishing effective controls over electronic payments, including the payment information on file for vendors and employees, to protect electronic payments from internal and external threats.

Our audit found the City did not have adequate internal controls over electronic payments to protect public funds. Specifically, in 2025 the City reported a phishing incident related to misappropriation of public funds that occurred in 2024. The City made a payroll payment totaling $7,158 to a fraudulent bank account.

We examined the City's controls over electronic payroll payments and found:

- Although the City had a policy in place requiring verification of bank change requests, the policy did not contain the required elements prescribed in the *Budgeting, Accounting and Reporting System* (BARS) Manual 3.8.11.30
- City staff did not consistently or adequately follow their intended procedures
- Training provided to City employees was not effective, as staff missed key red flags common to phishing schemes

We recommend the City:

- Develop written policies and procedures over electronic payroll payments to include the required elements prescribed in the BARS Manual (3.8.11.30). The City's policy should avoid procedures that rely on information coming through email, which is a communication medium traditionally vulnerable to unauthorized access.
- Provide adequate communication and training to staff on the verification requirements to ensure they consistently follow them.