Overview

State law (RCW 43.09.185) requires all state agencies and local governments to immediately report known or suspected losses of public funds or other illegal activity to the Office of the Washington State Auditor (SAO).

In 2022, the law was changed and requires the SAO to establish policies that further define the loss reporting process.

Reporting Requirements

Known or suspected losses or illegal activities are required to be reported immediately to the Office of the State Auditor.

All known or expected losses should be reported unless they have been specifically listed in the Losses or Illegal Activities Exempt from Reporting Requirement in this policy manual. The policy manual will have additional information specific to different state and local governments.

If after reviewing this manual and you still have questions, please report the loss and we can help determine if you need to report it or you can also reach us at: fraud@sao.wa.gov

Section 1 - Losses or Illegal Activities Exempt from Reporting Requirement

The following is a list of losses or illegal activities that state agencies and local governments are NOT required to report to the SAO:

- Normal and reasonable "over and short" situations from cash receipting operations. Record these transactions in the accounting system as miscellaneous income and expense, respectively, and monitor this activity for any unusual trends.
- Reasonable inventory shortages identified during a physical count. Record inventory adjustments in the accounting system.
- Unauthorized credit card attempts and/or transactions that are determined fraudulent by the bank and refunded.
- Breaking and entering or vandalism of property, including assets stolen out of government vehicles
- Loss of cellphones, tablets, laptops valued under $1,000 and not containing confidential data.
- For schools and libraries, laptops or iPads checked out by students or patrons, but not returned.
- Non-Sufficient Funds (NSF) checks accepted by the government
- Counterfeit currency accepted by the government (please report these to the FBI)

Section 2 – Clarification of losses to report Cybersecurity Incidents

State agencies and local governments must report cybersecurity incidents that involve the finances or financial records in some way. Below are some examples of activity you must report:

- Your government experiences a ransomware attack and makes a payment to the criminal actors to regain access to your data, even if your insurance company either pays the ransom or reimburses your government for the payment. This extortion payment is a financial loss as a result of illegal activity.
- Your government falls victim to a ransomware attack. You can restore your data from backups and do not pay the ransom. You should report this incident if it's possible the attackers accessed any financial records. Keep in mind that even though attackers may have only encrypted non-financial records, they could have accessed financial records and are waiting to ransom them at a later point. Determining which records the attackers accessed involves more than simply evaluating which records the attackers ransomed.
- Your staff relies on a fraudulent email to change banking information and an electronic payment is sent to a criminal, instead of to a vendor or employee, even if your insurance company covers the loss, or the bank is able to recover your funds.
- Someone gains unauthorized access to your computer system and they may have accessed your financial records, even if those records were not harmed or impacted in any way.
- You have a security incident that might have impacted your financial records or systems, but you are not certain.