ARIZONA Auditor General
Making a Positive Difference

FRAUD PREVENTION ALERT
Computer Tampering Frauds
November 2023

Why are we issuing this alert?

From 2015 through 2022, we issued 12 financial investigation reports associated with about $1.4 million of Arizona public money losses where computer tampering was either the means of theft and/or the instrument used to conceal theft. Pursuant to Arizona law, computer tampering frauds involve knowingly altering, damaging, deleting, or destroying computer data.[1] This alert outlines how some of these computer tampering frauds related to payroll disbursements, nonpayroll disbursements, and cash receipts occurred and what actions management can take to deter and detect them.

Theft, payroll disbursements—For over 1 year, a school district payroll technician manipulated the district's payroll software data by deleting her used leave hours, thereby converting those hours to unused leave. As a result, the district paid her $1,600 in wages and associated employee-related expenses she was not entitled to have when she used 77 hours of leave she had not earned but were reflected in her falsely inflated leave balance.[2]

Theft and concealment, payroll disbursements—For almost 2 years, a school district payroll specialist altered the district's payroll software data to stop her payroll deductions for health insurance premiums totaling $7,791, thereby increasing her take-home pay while still maintaining the benefits of district-provided health insurance. When district officials noticed discrepancies with her health insurance, she attempted to conceal her theft by again altering the payroll software data but this time to start her payroll deduction for health insurance premiums.[3]

Theft and concealment, cash receipts and nonpayroll disbursements—For over 2.5 years, a school district business manager falsified or omitted information in district accounting software, making it falsely appear as if 13 district-issued checks totaling $23,977 were actually issued and paid to authorized district payees and 28 check payment receipts totaling $14,356 were never received by the district. In fact, these 41 district-related checks totaling $38,333 were deposited into her personal bank accounts.[4]

Theft and concealment, nonpayroll disbursements—For 5.5 years, a water improvement district accounting manager issued 32 district checks and warrants with forged signatures totaling $524,686 payable to herself and to 3 businesses for which she managed the bank accounts. To help conceal her scheme, she recorded false payees, omitted payees, and deleted entries in the district's accounting software and in bank reconciliations.[5]

Why did this happen?

In each of the cases described above, district officials' failure to adequately separate duties was the primary factor leading to the fraudster's success.

---

[1] As described in Arizona Revised Statutes §13-2316, computer tampering violations range from class 6 to class 3 felonies and may also involve accessing, altering, damaging, or destroying any computer, computer system, or network; introducing a computer contaminant; and other reckless, disruptive, or illegitimate uses of a computer, computer system, or network.

[2] See Office of the Auditor General, *Glendale Elementary School District—Criminal Indictment—Theft, Misuse of Public Monies, Fraudulent Schemes, and Computer Tampering*, Report 22-404.

[3] See Office of the Auditor General, *Gadsden Elementary School District—Criminal Indictment—Theft, Misuse of Public Monies, Fraudulent Schemes, and Computer Tampering*, Report 21-403.

[4] See Office of the Auditor General, *Ray Unified District—Criminal Indictment—Theft and Misuse of Public Monies*, Report 19-408.

[5] See Office of the Auditor General, *Pine-Strawberry Water Improvement District—Criminal Indictment—Theft and Misuse of Public Monies*, Report 17-405.

Inadequate separation of duties enabled computer tampering frauds

Theft, payroll disbursements	Theft and concealment, payroll disbursements	Theft and concealment, cash receipts and nonpayroll disbursements	Theft and concealment, nonpayroll disbursements
District officials failed to adequately separate payroll responsibilities, allowing the payroll technician to alter her own records.	**District officials failed to adequately separate** payroll responsibilities, allowing the payroll specialist to change her own payroll data while also being responsible for notifying the insurance plan administrator of employee health insurance changes made outside of open enrollment, including her own, and further allowing her to reconcile payroll records to insurance billings.	**District officials failed to adequately separate** receipts and disbursements responsibilities, allowing the business manager to collect cash and check payments, make deposits, record expenditures in district accounting software, issue checks, act as an authorized signer on checks, receive bank account statements, and reconcile them to district accounting records.	**District officials failed to adequately separate** disbursements processing and recording, allowing the accounting manager to control check and warrant stock, prepare all checks and warrants, receive bank statements, record transactions in the district accounting software, and reconcile that information to the bank statements.

Recommendations

Trust is not a control. Adequate separation of duties deters fraud by eliminating the ability of one individual to perform enough steps in a process to steal and conceal. To that end, public officials and management should:

- Separate accounting procedures among employees so that authorization, recording, and custody functions are performed by different employees. For example, the employee preparing and recording checks should not maintain check stock and should not be an authorized signer. Additionally, the employee reconciling disbursements to bank records should not prepare or sign checks.
- Separate cash-handling functions from record-keeping functions, ensuring that an employee independent of cash-collection responsibilities totals sales from the system and another employee reconciles those sales to cash collections.
- Ensure payroll employees do not alter their own payroll records, and if the payroll software does not allow that restriction, review payroll software logs monthly to identify unauthorized changes in payroll employees' records.

To help identify computer manipulation for the purposes of concealment, public officials and management should:

- Review accounting software change logs monthly to identify unauthorized changes in check payee information.
- Compare canceled checks to accounting software records and supporting documentation to ensure all information is accurate and appropriate.
- Require accounting and payroll employees to take vacations during which time another employee performs key functions to deter and detect hidden and potentially fraudulent activities by the primary position holder.