



Washington State Auditor's Office

Troy Kelley

Independence • Respect • Integrity

Fraud Prevention & Internal Controls

April 2012

Agenda

- Fraud trends
- Case studies and internal controls
 - Payments
 - Credit cards
 - Gas card purchases and fuel misappropriation
 - Payroll
 - Cash receipting
- By the end of the session, we hope you will understand:
 - How to identify red flags
 - Why effective internal controls and monitoring are crucial
 - What to do if fraud happens at your entity

2011 Fraud Program statistics

During 2011, State and Local governments reported 427 known or suspected losses to our Office, totaling at least \$3,192,455.

Area	Number of losses	Amount of known loss
Loss of assets/property	183	\$966,746
Payments/credit cards	77	\$1,145,151
Cash-receipting	66	\$197,430
Payroll/benefits	23	\$416,309
Other/ethics	78	\$466,819

Fraud Program 2011 Highlights

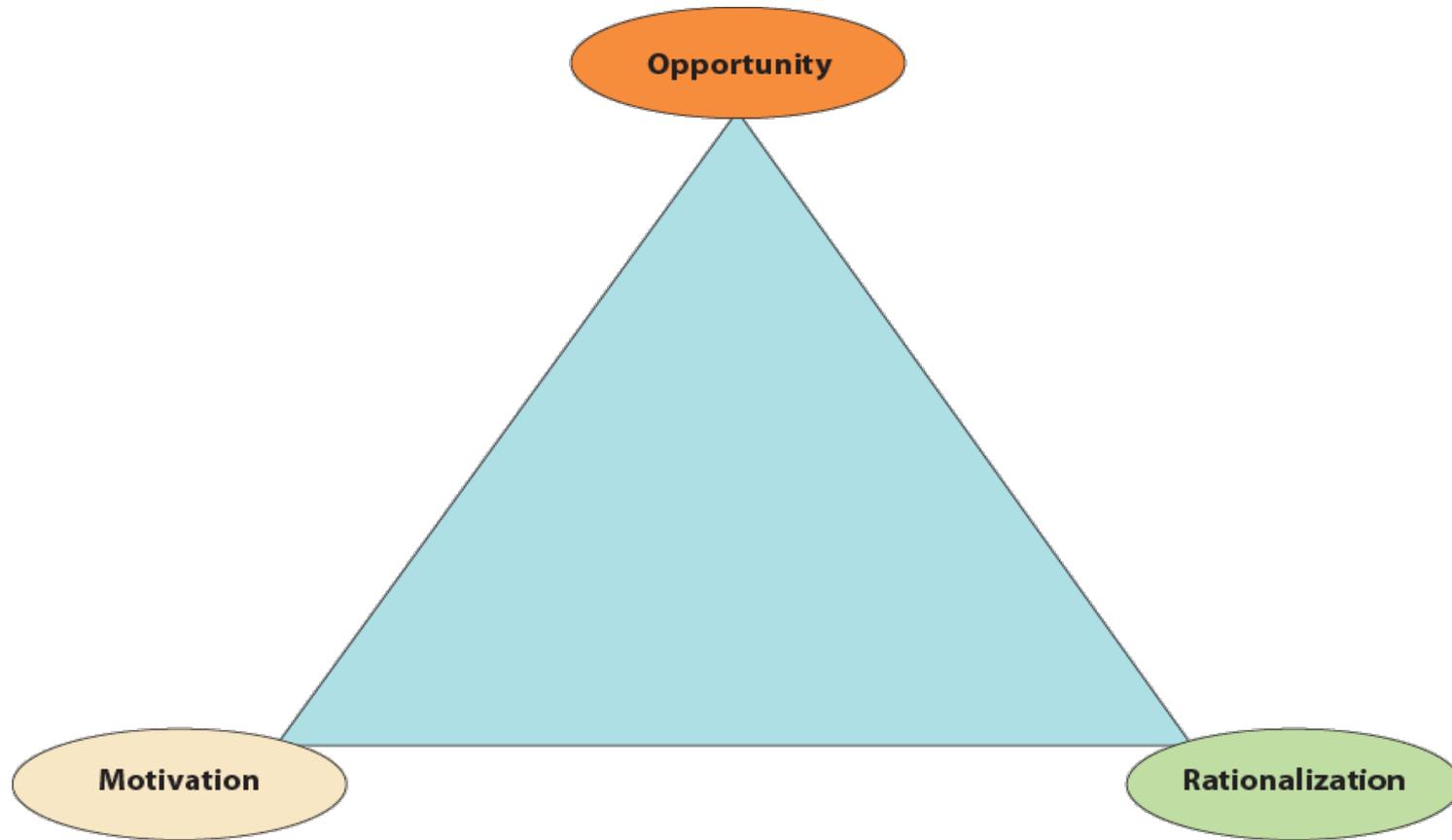
- In 2011, we reported on 50 frauds totaling \$1,352,396.
- Some of the larger investigations are:
 - Seattle School District - \$280,005
 - Birch Bay Water District - \$468,840
 - University of Washington - \$252,059

Fraud report history

Year	Cases	Amounts
1987	32	388,936
1988	26	451,122
1989	31	358,654
1990	15	120,121
1991	15	264,027
1992	20	266,629
1993	18	642,439
1994	30	903,304
1995	37	689,080
1996	48	958,805
1997	33	1,540,368
1998	31	597,479
1999	42	1,047,113

Year	Cases	Amounts
2000	30	167,363
2001	68	484,060
2002	56	1,122,328
2003	62	2,253,394
2004	47	331,803
2005	57	258,960
2006	33	611,711
2007	24	1,722,207
2008	35	548,855
2009	53	2,055,775
2010	75	1,864,652
2011	50	1,352,396
Total	968	\$20,961,581

The Association of Certified Fraud Examiners Fraud Triangle



Synonyms for internal controls?

If you do not care for the term internal controls, please substitute one of the following:

- Checks and balances
- Fraud prevention measures
- Review/monitoring system
- Fraud detection technique
- Accounting best practices
- Fraud deterrence

What are internal controls?

In accounting and auditing, internal control is defined as a process effected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives. ~COSO

It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in preventing and detecting fraud and protecting the organization's resources, both physical (e.g., machinery and property) and intangible (e.g., reputation or intellectual property such as trademarks). ~From Wikipedia

Why are internal controls important?

Effective internal controls

- Safeguard public funds
- Protect employees
- Assist in fraud prevention

Designing internal controls

- It is management's responsibility to design effective internal controls
- It is management's responsibility to ensure internal controls are operating as designed
- When designing/establishing internal controls break the system into segments and for each consider:
 - Will I be able to identify a loss? Will I identify the entire loss?
 - Will I be able to identify who is responsible?
- Cash-receipting example

Designing internal controls

- What makes auditor's cringe?
 - Auditor question: "How do you ensure all of the funds make it to the bank?"
 - Response: "Joe takes the money to the bank. He has worked here for 32 years. We trust him."
- Beware of "trusted employee syndrome"
- When designing internal controls don't forget the top of the organizational chart
 - Who typically has the easiest access to the most money?

Payments

- Accounts payable/vouchers
- Manual warrants
- Electronic transfers
- Employee reimbursements
- “Other” accounts
 - Advance travel account
 - Revolving/Imprest account

Birch Bay Water and Sewer District

Washington State Auditor's Office

Fraud Investigation Report

Birch Bay Water and Sewer District
Whatcom County

Report No. 1005868

Issue Date
June 20, 2011



WASHINGTON
BRIAN SONNTAG
STATE AUDITOR

Birch Bay Water and Sewer District

Summary

- Advance travel account
- Our investigation covered January 1, 2003 to December 31, 2010
- Misappropriation totaled at least \$468,840
- The former Treasurer pleaded guilty and was sentenced Thursday, Aug. 11, in Whatcom County Superior Court to three years in prison and restitution of \$450,000 to the District.

Birch Bay Water and Sewer District

How was it detected?

- During our audit of the District's financial statements, we identified several unusual transfers between two of the District's bank accounts.
- The unusual transfers were from the District's general checking account to its advance travel account, which has an authorized balance of \$2,000. The transfers we identified ranged from \$10,000 to \$58,900, well above that account's \$2,000 limit.
- The District Treasurer provided us with the bank statements for this account except the months in which we found the unusual transfers.

Birch Bay Water and Sewer District

What did we find?

- The District obtained bank records back to February 2003 for the advance travel account. From those records, we identified \$468,840.46 in misappropriated funds over eight years.

Year	Amount	Number of payments
2003	\$38,590.76	4
2004	\$37,361.36	8
2005	\$49,653.00	13
2006	\$66,911.38	19
2007	\$58,893.49	16
2008	\$79,136.98	19
2009	\$79,393.49	19
2010	\$58,900.00	15
Total	\$468,840.46	113

Birch Bay Water and Sewer District

Where did the money go?

- We identified unauthorized payments to 19 credit cards totaling \$326,480; a church, totaling \$21,050; the Treasurer, totaling \$116,309; and the Treasurer's wife, totaling \$5,000. The Treasurer signed all the checks.
- The credit cards paid from the advance travel account were in the Treasurer's name or his wife's name, except for one card the Treasurer opened in the District's name.
- All purchases on the cards were for personal items, such as airline tickets, lodging, groceries, shopping and restaurants.

Birch Bay Water and Sewer District

How was the fraud concealed?

- The Treasurer concealed the fraud in the accounting records by making journal entries that transferred cash to several construction projects.
- These journal entries were not supported by any documentation and were not relevant to any construction project.
- The District had established a review of journal entries starting in fiscal year 2009; however, the reviewer lacked the knowledge and understanding of the accounting system and coding to provide adequate oversight of the process.

Birch Bay Water and Sewer District

Lessons learned

- The former Treasurer was as trusted employee. He worked for the District for over 20 years.
- We found the Treasurer had full access to transfer funds between District bank accounts.
- He also had unrestricted access to the advance travel checkbook and was a signer on the account.
- The District did have a review process for bank statements; however, the review was not detailed and did not ensure that all bank statements were reviewed every month.

Washington Association of County Officials

Washington State Auditor's Office
Fraud Investigation Report

Washington Association
of County Officials
(WACO)
Thurston County

Investigation Period
August 1, 2006 through July 31, 2011

Report No. 1007456

Issue Date
March 27, 2012

 WASHINGTON
BRIAN SONNTAG
STATE AUDITOR

Summary

- Payments
- Our investigation covered August 1, 2006 to July 31, 2011
- Misappropriation totaled at least \$73,086

Washington Association of County Officials

How was it detected?

- The Association's Executive Director retired in June 2011. The newly hired Executive Director reorganized and reduced the Association's staffing structure.
- We were contacted by the Association's new Executive Director who found possible irregularities in the accounting system.
- We found the former Financial Operations Manager had written and printed five checks to herself totaling \$4,957.

Washington Association of County Officials

What did we find?

- We compared information from the Association's accounting system to the actual redeemed checks dating back to 2006. We found checks totaling \$67,086 that the former Financial Operations Manager wrote to herself, endorsed and deposited into per personal account.
- We found \$6,000 was misappropriated from the Association's non-profit scholarship fund using the same method.

Year	Amount
2007	\$2,714.37
2008	\$21,694.23
2009	\$28,924.17
2010	\$14,957.15
2011	\$4,957.15
Total	\$73,086.19

How was the fraud concealed?

- The former Financial Operations Manager wrote checks to herself and then either voided the checks or changed the vendor names in the accounting system.
- Some signatures on the check were not authentic. Each of five checks written in 2011 contained the signatures of the new Executive Director, who examined the signature and stated he had not signed the checks.

What happened to the employee?

- Law enforcement officers informed our Office the former Financial Operations Manager stated she had misappropriated funds but not forged signatures.
- The former Financial Operations Manager faces charges of first-degree theft and will be arraigned in Thurston County Superior Court.

Washington Association of County Officials

Lessons learned:

- The former Financial Operations Manager was given complete and exclusive control of the Association's finances with almost no oversight or independent review.
- The former Executive Director signed blank checks for the former Financial Operations Manager with no review of the supporting documentation.
- During Association conferences, cash and checks for the scholarship fund were handed to the former Financial Operations Manager who did not account for the money with donor receipt or any other method.

Tacoma-Pierce County Employment Training Consortium

Washington State Auditor's Office

Fraud Investigation Report

**Tacoma-Pierce County Employment and
Training Consortium
(WorkForce Central)**

Report No. 1006149

Issue Date
September 12, 2011



WASHINGTON
BRIAN SONNTAG
STATE AUDITOR

Summary

- Payments
- Our investigation covered June 2009 to April 2011
- Misappropriation totaled at last \$52,382.24

How was it detected?

- The Consortium Accounting Technician while paying approved invoices, noticed a fictitious vendor.
- Further review of the account indicated that an invoice had been paid and voided.

What did we find?

- The former CFO created a fictitious vendor and invoice from that vendor and authorized \$52,382.24 electronic payment to his personal bank account.

How was the fraud concealed?

- The former CFO created a vendor and a fictitious invoice and authorized payment.
- He attempted to alter and/or delete the transaction from the accounting system.

What happened to the employee?

- Former CFO's CPA license was revoked.
- A find of \$5,000 plus \$1,000 investigative and legal costs was assessed by the Washington State Board of Accountancy.
- Case was referred to the Thurston County Prosecuting Attorney.

Lessons learned:

- The former CFO supervised and had access to the accounts payable, payroll and all other accounting functions.
- He was also responsible for performing bank reconciliations and reviewing payroll and vendor reports before checks were issued.

Payment Internal Control

- Scanned documents, know what you are looking for
- Review bank reconciliations in a timely manner
- Ensure voided transactions are truly voided
- Only pay original invoices
- Ensure payments made outside normal process are approved, supported and for public purpose
- Establish policies and procedures and ensure they are enforced (practice = policy)

Payment Internal Controls

- Review vendor lists for unusual vendors or excessive payments (W-9's/confirmations)
- Review for transactions that are out of the ordinary
- Look for unusual or excessive reimbursements to one employee
- Ask questions and get a supported answer. Confirm with a third party if necessary
- Create and review error reports (example: same bank account number or address)
- Look for unusual journal entries, such as entries to cash

Payment Internal Controls

- Review for inventory discrepancies. Verify inventory records reconcile with purchases and use.
- Know the “universe” of what you are reviewing.
- Lock up unsecured check stock.
- Require detailed expense reports with original receipts and documentation attached.
- Review employee reimbursements for expenses claimed on days the employee did not work.
- Look for payments or employee reimbursements approved by someone outside the department. These are high risk.

Payment Internal Controls

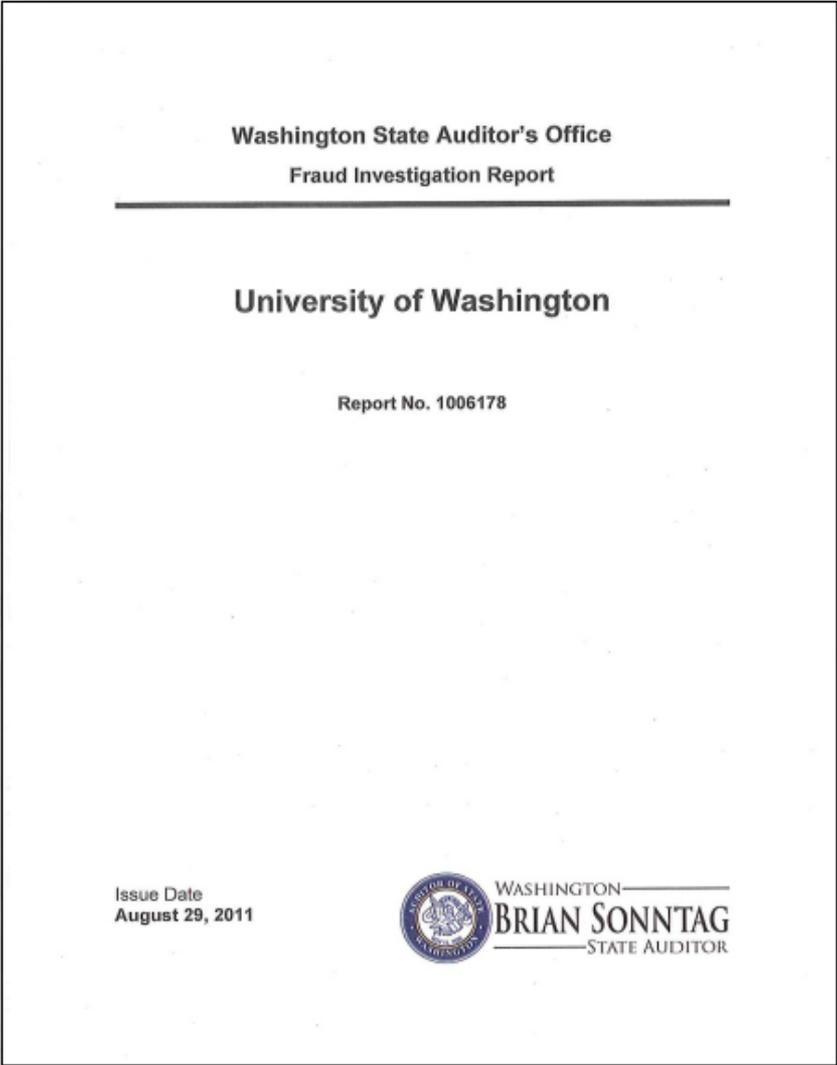
- Ensure items purchased were received and are on-site.
- If you use positive pay, make sure you know what the bank is verifying.
- Preliminary vs. final reports: know what you are reviewing.
- Call your software company and inquire about known system weaknesses (ability to change vendors/payees after entry, inability to detect duplicate payments, etc.)
- Review for expenses that end in round numbers.

Payment Internal Controls

- Review accounts payable transactions for excess good and services.
- Have an expectation of reasonable expense and compare it to actual payments entered into the system and what cleared the bank.
- Look for unusual endorsements.
- Review for expenses that exceeded budgeted amounts or prior year totals.
- Warrants/checks should never go back to the department or person that initiated the payment.

Credit card expenditures

- Travel
- Personal purchases
- Purchase/returns
- Abuse of power



Summary

- Procurement card and travel purchases, duplicate reimbursements and unearned leave
- Investigation covered June 2008 to August 2010
- Misappropriation totaled at least \$252,059

How was it detected?

- Management noticed unusual transactions on the Department's Corporate Travel Account while the former employee was on vacation. It determined the charges were personal charges.

What did the University find?

- The former Administrative Manager used a University-issued procurement card and department corporate travel account for personal use.
- He falsified records and requested reimbursement for personal travel and previously reimbursed expenses to another individual.
- He falsified documents to give the appearance he had paid the travel expenses for another individual. However, the other individual paid his own travel expenses and was already reimbursed by the University.
- He was paid for 201 hours of annual leave that he had not earned.

What did we find?

- We reviewed the University's investigation and agree with its conclusion.
- The former employee misappropriated funds using the following methods.

Method	Amount
Procurement card purchases	\$204,340
Travel card purchases	\$39,350
Reimbursements for personal or already reimbursed charges	\$1,612
Unearned leave	\$6,757
Total	\$252,059

How was the fraud concealed?

- The former Administrative Manager's job responsibilities were not segregated. He was responsible for approving, processing, monitoring, and reconciling transactions which included procurement card and corporate travel charges.
- The former employee circumvented controls by sending a falsified email to the University's procurement card office on behalf of the Chief Financial Officer of the Medical Center requesting an increase to his procurement credit limit.
- The University's online procurement card system allowed any authorized user to perform both the cardholder and reconciler certification that charges were appropriated. As a result, the Administrative Manager routinely performed both certifications.

What happened to the employee?

- Former employee was charged with seven counts of first-degree theft and 12 counts of second-degree theft.
- At the time of hire, the former employee was facing felony theft charges in King County related to a 2004 incident in which he was alleged to have purchased \$1,073 in artwork using cancelled credit cards.

Lessons learned:

- The Medical Center Administration did not sufficiently oversee and review the Administrative Manager's procurement card activities.
- No one reviewed or reconciled his procurement card or travel purchases to supporting documentation.
- The Administrative Manager's job responsibilities were not segregated. He was responsible for approving, processing, monitoring, and reconciling transactions.
- Department should require employees to submit leave slips when taking time off and ensure that the leave is recorded on the timesheets, reconciled to leave slips and deducted from leave balances.

Credit card internal controls

- Scanned documents
- Only pay original invoices
- Ensure payments made outside normal process are approved, supported and for public purpose
- Establish policies and procedures and ensure they are enforced (practice=policy)
- Review credit card bills and support documentation to ensure the purchases are approved, supported and for public purpose
- Take a step back and look at your credit card use. Is it appropriate and necessary?

Gas card purchases and fuel misappropriation

- Cards that were never cancelled
- Personal use
- “Family and friends”
- Unsecured cards

Town of Cathlamet

Washington State Auditor's Office
Accountability Audit Report

Town of Cathlamet
Wahkiakum County

Report Date
July 21, 2011

Report No. 1006117

Issue Date
September 12, 2011



Summary

- Fuel card
- Our investigation covered January 1, 2007 to September 30, 2010
- Misappropriation totaled at least \$7,705

How was it detected?

- A Fire Department volunteer noted that only unleaded fuel had been purchased on one fuel card from March 2008 through August 2010.
- This activity was unusual since the Department had only one vehicle that used unleaded fuel, a seldom used back-up vehicle.
- We were contacted by the Town Clerk-Treasurer about the potential loss.

Town of Cathlamet

What did we find?

- The Department opened four credit cards without approval from the Town Council. Department volunteers stated one card had been missing since March 2008, but was not de-activated. Only unleaded fuel, totaling \$7,705.18, had been charged to card number 7 between March 2008 and September 2010.
- The majority of unleaded fuel purchases were made on missing card number 7.

Unleaded fuel by card	
6	\$1,826.09
7	\$8,259.75
8	\$1,299.27
10	\$1,229.03
Total	\$12,614.14

Town of Cathlamet

What did we find?

- The Department maintains 10 vehicles that include fire engines and ambulances that all use diesel fuel. The Department has only one rescue vehicle and various small items of equipment that use unleaded fuel.
- Unleaded fuel purchases from January 2007 through September 2010 were unreasonable compared to diesel purchases. Based on the accessibility of the cards, it is difficult to quantify the exact amount of fuel loss.

Period	Unleaded	Diesel fuel	Total
2007	\$983.89	\$3,253.07	\$4,236.96
2008	\$4,540.05	\$5,303.38	\$9,843.43
2009	\$3,764.12	\$3,814.13	\$7,578.25
2010	\$3,326.08	\$3,456.43	\$6,782.51
Total	\$12,614.14	\$15,827.01	\$28,441.15

How was the fraud concealed?

- The Department obtained four credit cards without approval from the Town Council.
- The Department did not have controls or monitoring in place to oversee fuel card use and did not review monthly credit card bills or require documentation to show that all fuel purchases were for a Department-related purpose.
- The Town did not have a formal policy regarding credit card use and monitoring.

What happened to the volunteer?

- The Town agreed to a settlement of \$6,000. The individual suspected in the loss pleaded guilty to felony second-degree theft and was sentenced to 35 days in jail.

Town of Cathlamet

Lessons learned:

- Fuel cards were left unsecured in the vehicles and shared by all department volunteers. They were not checked out nor were charges identified as related to any person or vehicle.
- Fuel invoices were paid using a departmental petty cash account and not reviewed and approved by Town Council or management prior to payment.
- No one independently reviews or monitors fuel charges on the cards.

Public Utility District No. 1 of Douglas County

Washington State Auditor's Office
Fraud Investigation Report

Public Utility District No. 1 of Douglas
County

Report No. 1006550

Issue Date
October 5, 2011



Summary

- Payments
- Our investigation covered April 20, 2006 to December 19, 2010
- Misappropriation totaled at least \$12,384.68

Public Utility District No. 1 of Douglas County

How was it detected?

- Two District fuel cards were missing in 2010.
- District management found fuel purchases charged to a missing fuel card.
- The District found the card had been used at the vendor's Wenatchee fueling station, which is outside of Douglas County, where most of the District's operations take place.

Public Utility District No. 1 of Douglas County

Where did the money go?

- In November and December of 2010, a video camera used by the vendor at the East Wenatchee station caught on tape a District employee fueling a personal vehicle during a weekend. The camera recorded one transaction in November and two transactions in December, totaling \$213.20.
- The District compared fuel purchases at the vendor to that employee's leave slips and non-scheduled work time and found 68 fuel transactions had taken place when the employee was not at work.
- A former District journeyman lineman admitted to using the District's missing card to fuel his personal vehicle.

Public Utility District No. 1 of Douglas County

What did we find?

- The District reviewed all transactions at the station going back to 2006 and found 251 questionable purchases totaling \$12,914.30
- We reviewed the District's investigation and examination of fuel card transactions. We found \$742.82 of the \$12,914.30 questionable purchases reported could not be traced to the specific employee.

Public Utility District No. 1 of Douglas County

How was the fraud concealed?

- The former employee started in the warehouse, which provided first-hand knowledge of the District's fueling procedures.
- His job responsibilities provided access to fuel cards kept in the vehicles in the District's parking lot.
- The employee worked at different times than other employees, providing the opportunity to use fuel cards kept in vehicles without the knowledge of District staff.
- District staff does not regularly inventory fuel cards. It only logs in new cards it receives due to expirations or a change in vendor.
- District staff did not match fuel card purchases to assigned vehicles.

What happened to the employee?

- The former employee was accused of first-degree theft, a Class B felony with a maximum penalty of 10 years in prison/or a \$20,000 fine.
- He was charged in May in Chelan County Superior Court. His trial is set for November 2012.

Public Utility District No. 1 of Douglas County

Lessons learned:

- The District writes the fuel card's PIN number on the outside of the card's sleeve and places it in the assigned vehicle.
- Employees do not retain or submit receipts for fuel purchases.
- No one reconciled between receipts and invoiced purchases.
- District department heads do not review and initial vehicle log sheets monthly.
- Employees were not trained in the appropriate use of fuel cards and in documentation requirements.

Gas card/fuel misappropriation internal controls

- Review for inventory discrepancies. Verify inventory records reconcile with use.
- Look for fuel purchases at locations or times of the day that do not make sense given the department's operations.
- Review fuel purchase for type of fuel or grades that do not meet the department's needs.
- Look for frequent purchases or unusual trends by individuals assigned gas cards.
- Contact fuel vendors and inquire about options to restrict access after certain hours or locations.

Gas card/fuel misappropriation internal controls

- Reconcile fuel purchases to use (mileage logs) for credit purchases and supply tanks.
- Determine if you can assign responsibility for fuel losses.

Payroll

- Extra payroll checks
- Leave buyouts
- Not reducing leave balance by amount of leave taken
- Ghost employees
- Benefits

Ridgefield School District No. 122

Washington State Auditor's Office
Special Investigation Report

Ridgefield School District No. 122
Clark County

Report Date
March 2, 2010

Report No. 1003233

Issue Date
March 15, 2010



Summary

- Payroll
- Our investigation covered July 1999 to April 2009
- Misappropriation totaled at least \$806,644

How was it detected?

- An outside organization requested an employee and salary verification for the former Assistant Business Manager.
- When questioned by District management about discrepancies with her salary, the former Assistant Business Manager admitted to manipulating her payroll.

What did we find?

- After preliminary payroll reports were generated, the former employee inflated her salary and expensed it across multiple line items before finalizing payroll. Once payroll was finalized, most of the final reports showing the fraudulent transactions were missing or destroyed.

How was the fraud concealed?

- The former Assistant Business Manager recorded misappropriated funds as several benefit expenses, thereby blending the falsified transactions into normal payroll expenses.
- She reduced her cumulative earnings in the accounting system so information on her year-to-date pay reflected her normal salary.
- She destroyed District final payroll reports that showed falsified transactions and replaced them with preliminary reports that were manipulated to look like final payroll reports.

What happened to the employee?

- The former Assistant Business Manager pleaded guilty to one count of felony wire fraud in U.S. District Court.
- She was sentenced to two years in prison followed by three years of supervised release and restitution of \$806,645 to the District.
- She forfeited her deferred compensation account, personal bank account, and personal property.

Lessons learned:

- The former employee was a trusted employee who had been with the District for more than 21 years as a Payroll Clerk and Assistant Business Manager.
- The former Assistant Business Manager had full control over payroll processing, unrestricted computer system access and authority to transfer District funds.
- District management provided limited oversight and monitoring.

Payroll internal controls

- Review payroll expenses for unusual fluctuations and amounts that are outside your expectation, including benefit line items and overtime.
- Use the straight-line approach for payroll processing.
- Review personnel files to verify it is a real person and they are an employee (ghost employees can be real people).
- Create and review error reports (example: same bank account number or address).
- Look for unusual journal entries.
- Know the “universe” of what you are reviewing.

Payroll internal controls

- Look for employees that rarely or never take leave.
- Review payroll reports for employees that use a P.O. Box.
- Review leave reports for reasonableness.
- Preliminary vs. final reports: know what you are reviewing.
- Call your software company and inquire about known system weaknesses.

Thurston County Cemetery District No. 2

Washington State Auditor's Office

Fraud Investigation Report

**Thurston County Cemetery District No. 2
(Yelm Cemetery)**

Report No. 1006182

Issue Date
August 29, 2011



WASHINGTON
BRIAN SONNTAG
STATE AUDITOR

Thurston County Cemetery District No. 2

Summary

- Cash receipts, credit card charges, and payroll
- Our investigation covered October 1, 2001 to April 30, 2011
- Misappropriation totaled at least \$62,068

Thurston County Cemetery District No. 2

How was it detected?

- Citizen contacted our Office with a concern that the Cemetery Superintendent was using District resources for personal use and was using public money to advertise his personal business.
- The Thurston County Treasurer's Office, which is the bank for the District, also informed us that the Superintendent was depositing personal checks into the cemetery account.

Thurston County Cemetery District No. 2

What did we find?

- We found the Superintendent deposited District funds into his personal checking account. When he did deposit money due to the District, he would use a personal check and did not deposit the full amount into the District's account.
- In addition, the Superintendent gave himself an unauthorized pay increase, employee benefits and credit card reimbursements.

Method	Amount
Cash receipts not deposited	\$41,925
Credit card reimbursement double payments	\$1,011
Unauthorized pay increase	\$1,612
Unauthorized employee benefit payments	\$17,520
Total	\$62,068

Thurston County Cemetery District No. 2

How was the fraud concealed?

- The former District Superintendent kept two sets of receipt books. One set belonged to the District. He used the other for his monument and headstone business.
- He deposited District funds in a personal checking account then used personal checks to deposit District funds with the County Treasurer. However, he did not deposit the full amount due to the District in its account.

Thurston County Cemetery District No. 2

What happened to the employee?

- The former District Superintendent was terminated.
- Investigation were forwarded to the Thurston County Prosecuting Attorney's Office.

Thurston County Cemetery District No. 2

Lessons learned:

- Former District Superintendent used the cemetery office and ground for both District business and his personal business.
- There was a lack of Board oversight and monitoring.
- The District had no formal policies and procedures in place to cover daily operations such as cash receipting, purchases, employee reimbursement, credit cards, and payroll. It operated on verbal agreements.

Summary

- Cash receipting
- Our investigation covered January 1, 2005 to January 4, 2011
- Misappropriation totaled at least \$62,150

How was it detected?

- The County employee in charge of reconciling Probation Services cash receipts to bank deposits identified that the funds had not been deposited.

What did we find?

- Probation fees of at least \$51,816 paid between November 22, 2010 and January 4, 2011 were not deposited.
- An additional \$30,772 in voids and cash shortages were not supported by County records.
- Checks totaling \$10,334 were substituted for cash removed from the deposit.
- The County did not have records to support \$734,894 in adjustments to customer accounts.

How was the fraud concealed?

- One employee was responsible for collecting and reconciling daily cash receipts and making bank deposits.
- Bank deposits were not made within 24 hours as required by state law (RCW 43.90.240).

What happened to the employee?

- Formal charges of felony theft, misdemeanor theft and misappropriation of accounts by a public officer were filed.

Lessons learned:

- The former employee had complete access to key systems, including cash-receipting, bank deposits and account adjustments.
- No one independently monitored cash/check composition or adjustments.
- No one reconciled the system transactions, manual receipts or collection agency payments with the bank deposits.

Cash receipting internal controls

- Compare bank deposits to cash receipt records and verify the mode of payment agrees.
- Review voided transactions to ensure they are supported and legitimate.
- Perform surprise cash counts.
- Get a handle of unanticipated revenues.
- Look for missing deposit slips.
- Look for unusual void activity by employee or department.

Cash receipting internal controls

- Create and review error reports
- Look for unusual journal entries
- Follow up on unusual over/short cash receipting activity
- Review for inventory discrepancies. Verify inventory records reconcile with use
- Look for deposits not made daily or intact
- Cash deposits differ from normal patterns
- Know the universe of what you are reviewing

Cash receipting internal controls

- Preliminary vs. final reports: know what you are reviewing.
- Call your software company and inquire about known system weaknesses (receipt posting dates, ability to reprint receipts, etc.)
- Look for negative cash receipts.
- Look for billing and credit adjustments.
- Look for hidden rows/columns.
- Know who is receiving the billing compliant calls

Cash receipting internal controls

- Safeguard and limit access to receipts awaiting deposit. How long has it been since the safe combination was changed?
- Perform a periodic “look back” of revenues. Do they make sense given your understanding of the operations?
- Review receipt sequence. Are receipts used in sequential order? Are all the receipt numbers accounted for?
- Review bank reconciliations. Are they timely? Do reconciling items make sense? Why so many outstanding items?

Cash receipting internal controls

- Spot check customer accounts, such as utilities. Are payments posted timely to the correct account in the correct amount?
- Customer billings should detail the prior balance, payments made, adjustments to the account and the current amount due.
- Review security deposit refunds.
- Review employee account activity.

Fraud prevention

- Segregation of duties
- Mandatory vacations
- Let them know you are looking
- Cross train duties
- Establish strong policies and ensure staff are trained

Our Office's client support program

- Can be found on the State Auditor's Office website, www.sao.wa.gov under the Client Support tab.
- Contains a section on fraud prevention and internal controls.
- Show best practices and other resources in fraud prevention.
- Is part of our on-going effort to provide fraud prevention information to our audit clients.

Fraud happens

What to do if it happens to you:

- Immediately notify the State Auditor's Office on the web at www.sao.wa.gov
- Protect accounting records from loss or destruction
- Don't enter a restitution agreement with an employee (Auditor/Attorney General approval required)
- Ensure personnel action taken for violating policies and procedures, not for misappropriating public funds
- File a police report (consult our Office on timing)
- Change bank account access (credit cards, too!!)

Fraud happens

What to do if it happens to you:

- Do not try to be the investigator. But do start a record: how it came to your attention, records and conversations, etc.
- Do not physically prevent an employee from leaving the room or leaving the building.
- Do not agree to let the employee repay money and it will all go away.

Summary

- Remember the fraud triangle
 - You control the opportunity
- When designing internal controls, break down the system into segments and analyze:
 - If you could identify a loss
 - If you could identify who is responsible
- Beware of the “trusted employee” trap
 - Who has the most access to funds?
 - Sometimes good people do bad things
- Remember our Office doesn't review every transaction. Don't rely on auditors to find the fraud. That is your job!

Contacts

Troy Kelley

State Auditor

(360) 902-0360

Troy.Kelley@sao.wa.gov

Sarah Walker

Fraud Manager

(360) 480-1103

Sarah.Walker@sao.wa.gov

Website: www.sao.wa.gov