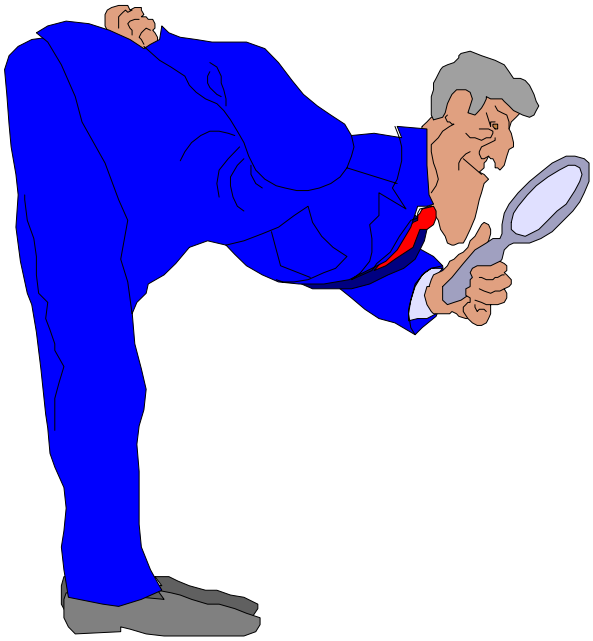
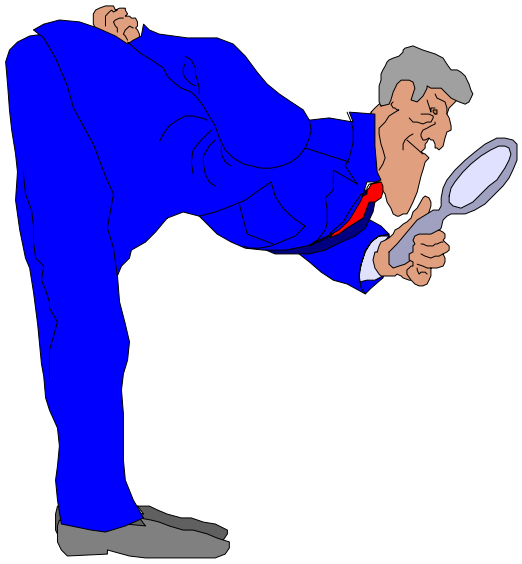


Fraud Detection and Development

Joseph R. Dervaes, CFE, CIA
Audit Manager for Special Investigations
Washington State Auditor's Office

January 2004



Additional Course Materials

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

Introduction

Fraud Audit Program
Statement on Auditing Standards No. 53
Statement on Auditing Standards No. 82
Association of Certified Fraud Examiners Report to the Nation
Citizen Expectations
Fraud Audit Program
Two Major Types of Risk for Fraud
Reporting Losses of Public Funds or Assets or Other Illegal Activity
Critical Actions Checklist for New Fraud Cases
State of Washington Fraud Statistics
Fraud Statistics by Area
Fraud Statistics by Entity Type
Fraud Case Analysis
The Average Fraud
Fraud Detection Information
State of Washington Trial Record
Primary Goals in Fraud Development
Conclusions of Case Studies
Reasons Auditors Fail to Detect Fraud
Types of Fraud
Types of Fraud Perpetrators
Fraud Interaction Factors
Fraud Perpetrator Characteristics
Causes of Fraud
Consistent Patterns in Fraud Cases
The System of Internal Control
Key Internal Controls for Managers (And Auditors)
Emerging Fraud Trends
Four Troublesome Internal Control Areas for Fraud
Methods Used to Launder Entity Revenue and Disbursement Checks
Twenty Danger Signs of Embezzlement
Forty Common Forms of Fraud
Twenty-Five (25) Life Rules
Summary

General Fraud Information

Definitions
Fraud Detection Methods - General
Fraud Detection Methods - Cash Receipts
Fraud Detection Methods - Cash Disbursements

Cash Receipt Fraud Schemes

Cash Disbursement Fraud Schemes

Purchasing and Contracting Fraud Schemes

Additional Course Materials

BIOGRAPHY

JOSEPH R. DERVAES, CFE, CIA
AUDIT MANAGER FOR SPECIAL INVESTIGATIONS
WASHINGTON STATE AUDITOR'S OFFICE

Joe is the Audit Manager for Special Investigations at the Washington State Auditor's Office where he is responsible for managing the agency's Fraud Program. He specializes in employee embezzlement fraud within all state agencies (170) and local governments (2,400) in the state of Washington. He monitors all fraud audits throughout the state and has participated in the investigation of approximately 600 cases involving losses of over $12.2 million in the past 17 years.

Joe received his Bachelor of Science Degree from the University of Tampa (Florida) in 1963 with majors in both accounting and business administration. He completed graduate studies at Air University, Maxwell Air Force Base, Alabama, in Comptrollership (1975) and Military Science (1977). He is a Certified Fraud Examiner (CFE), a Certified Internal Auditor (CIA), and a retired United States Air Force Lieutenant Colonel. His audit experience includes 20 years with the Air Force Audit Agency and 20 years with the Washington State Auditor's Office.

Joe is the fraud audit training instructor for the Washington State Auditor's Office, and the author of the agency's “Fraud Audit Manual”, and the following agency training courses: “Fraud Detection and Development”, “Fraud Auditing Update”, “Computer Fraud”, “Cash Count Procedures”, and “Interviewing Techniques”. He received the agency’s “Outstanding Employee Award” in 1986, 1988, and 1999 (2).

Joe is very active in the Association of Certified Fraud Examiners (CFE). In 2003, he received the Association’s coveted Donald R. Cressey Award for his lifetime contributions to fraud detection, deterrence, and education. He is a Life Member, Fellow, Member of the Board of Review, Regent Emeritus, and an adjunct faculty member. He is also the author of the Association’s "Cash Receipts and Disbursements" fraud training course, and a contributing author of the Second Edition of the "Fraud Examiners Manual". He received the Association’s “Distinguished Achievement Award” in 1995. As a nationally recognized author, Joe’s profile and articles on “Big Switch: The Check-for-Cash Substitution Scheme”, “Cash Disbursement Frauds -- Treasury Funds Are The Target”, “All Wired Up -- Electronic Funds Transfers are Prime Fraud Targets”, and a regular “By-Line Column on Fraud’s Finer Points” have been published in the “The White Paper”, the Association’s international magazine. He is also the founding President of the Pacific Northwest Chapter of the Association and a frequent speaker at chapter fraud seminars and conferences.

Joe writes "Fraud Tips" articles for the newsletter of the Association of Public Treasurers of the United States and Canada, is a member of the Accounting, Automation, and Internal Controls Committee, and received the organization’s Service Award for 1996. He is the author of the Association's manual on "Techniques for Identifying and Preventing Fraudulent Schemes" and helped develop its "Internal Controls Checklist".

Joe presents fraud awareness seminars to both auditors and management officials of governmental entities and professional associations throughout North America.

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

Introduction

Fraud Audit Program
Statement on Auditing Standards No. 53
Statement on Auditing Standards No. 82
Association of Certified Fraud Examiners Report to the Nation
Citizen Expectations
Fraud Audit Program
Two Major Types of Risk for Fraud
Reporting Losses of Public Funds or Assets or Other Illegal Activity
Critical Actions Checklist for New Fraud Cases
State of Washington Fraud Statistics
Fraud Statistics by Area
Fraud Statistics by Entity Type
Fraud Case Analysis
The Average Fraud
Fraud Detection Information
State of Washington Trial Record
Primary Goals in Fraud Development
Conclusions of Case Studies
Reasons Auditors Fail to Detect Fraud
Types of Fraud
Types of Fraud Perpetrators
Fraud Interaction Factors
Fraud Perpetrator Characteristics
Causes of Fraud
Consistent Patterns in Fraud Cases
The System of Internal Control
Key Internal Controls for Management (And Auditors)
Emerging Fraud Trends
Four Troublesome Internal Control Areas for Fraud
Methods Used to Launder Entity Revenue and Disbursement Checks
Twenty Danger Signs of Embezzlement
Forty Common Forms of Fraud
Twenty-Five (25) Life Rules
Summary

FRAUD AUDIT PROGRAM

Washington State Auditor's Office

Organization of the State Auditor's Office

- Created by the Constitution as the auditor of all public accounts
- Audit Services
    - State agencies (170)
    - Local governments (2400)
- One of few states which audits all state and local governments
- Largest accounting firm in the state (275 Assistant State Auditors)

Fraud audit program

- Entities are required to notify us when fraud is suspected or detected (Revised Code of Washington 43.09.185).

    General requirements:

    - Notify the State Auditor's Office when fraud or other irregularities are suspected or detected.
    - Protect the accounting records from destruction.
    - Don't make a restitution agreement with the suspect prior to an audit to establish
    - the amount of loss in the case.
    - File a police report when advised to do so by the State Auditor's Office.

- Continuing education program is foundation of the program
    - Agency training classes for all auditors
        - New Employee Orientation
        - Fraud Detection and Development
        - Fraud Auditing Update
        - Computer Fraud
    - Entity/Professional association awareness training seminars

Audit Manager for Special Investigations (2) manages program

- State-wide resources for all Assistant State Auditors and entities
- Serve as focal point for agency body of knowledge on fraud
- Monitor all fraud cases from birth to death
    - All fraud cases are referred for prosecution
    - Restitution includes the loss amount plus audit costs
- Purpose is to ensure that learning outcomes from prior fraud cases are employed in current fraud audits to preclude Assistant State Auditors from making costly mistakes.

STATEMENT ON AUDITING STANDARDS NO. 53

The Auditor's Responsibility to Detect and Report Errors and Irregularities (Fraud) Superseded by SAS No. 82

Requirements

- Assess the risk that fraud may cause the financial statements to contain a material misstatement
- Design the audit to provide reasonable assurance of detecting material fraud
- Exercise due professional care
- Exercise a high degree of professional skepticism
    - Assess tone at the top
        - ☞ Who's minding the store?
        - ☞ Does anyone care?

Major impact of SAS No. 53: Compliance with state laws and regulations

GAO Yellow Book: "In government audits, the materiality level and/or threshold of acceptable risk may be lower than in similar type audits in the private sector because of the public accountability of the entity, the various legal and regulatory requirements, and the visibility and sensitivity of government programs, activities, and functions."

State Auditor's Office exceeds the standards of SAS #53

- We audit on a cyclical basis and use the risk-based audit approach
-
- This includes identifying areas of high risk for fraud
-
- Specifically, the things included in this training course

Almost all fraud in government in Washington State is **not** material to the financial statements

The general public believes all fraud is important in government

- They hold Assistant State Auditors in the State Auditor's Office to a higher standard
- It's their tax dollars
- Materiality is not the issue for them
- Public officials must be good stewards of all funds, including spending dollars wisely and safeguarding funds from loss while in their custody and under their control.

The expectation gap is the difference between what the general public thinks, and what auditors believe, they are responsible for when it comes to fraud.

The Assistant State Auditor's purpose and role in government audits should be to close the expectation gap.

We use the concept that says: "There is no such thing as a small fraud, only a large fraud which has not had a sufficient amount of time to develop to its full potential."

STATEMENT ON AUDITING STANDARDS NO. 82
Consideration of Fraud in a Financial Statement Audit

Major Impact

What is SAS No. 82?

Provides guidance to auditors in fulfilling their responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement caused by fraud.

Specifically, the statement describes fraud, requires a risk assessment of a material misstatement due to fraud, and provides guidance on the auditor's response to the assessment, evaluation of test results, and auditor communication about fraud. It also describes certain documentation requirements.

Did SAS No. 82 affect the State Auditor's Office practices?

Only in the area of documentation requirements. The State Auditor's Office already far exceeds all other requirements put in place by SAS No. 82. We must make minor changes in the way we document our workpapers to comply with the standard; but, this is an issue of form rather than substance.

SAS No. 82 Highlights:

Fraud is intentional -- Errors are unintentional. The auditor's interest in fraud relates to acts that cause a material misstatement of the financial statements.

There are two types of fraud misstatements:

(1) **Fraudulent financial reporting**: The intentional misstatement or omission of amounts or disclosures in financial statements to deceive financial statement users.

(2) **Misappropriation of assets:** The theft of an entity's assets which causes the financial statements to be materially misstated.

During planning, the auditor must assess the risk of material misstatement due to fraud and consider fraud risk factors for each type of fraud.

Categories of risk factors to consider for **fraudulent financial reporting** are: (a) management characteristics and influence over the control environment; (b) industry conditions; and, (c) operating characteristics and financial stability.

Categories of risk factors to consider for **misappropriation of assets** are: (a) susceptibility of assets; and, (b) controls.

The risk assessment process is on-going and is a cumulative process.

The auditors response to the risk assessment may include changes to the overall engagement such as assignment of personnel or increased professional skepticism. The response may also be focused at an account balance or assertion level which may include changing the nature, timing, or extent of planned tests.

The auditor should evaluate the test results and take appropriate steps if a material or possible material misstatement due to fraud has been detected, including: (1) considering the implication for other aspects of the audit; (2) discussing the matter and the approach with senior management; (3) obtaining additional evidence, if needed, and evaluating the effect on the financial statements and the auditor's report; and, (4) suggesting the client consult with legal counsel.

Documentation in the **audit plan** should provide evidence of the performance of a risk assessment. If risk factors are present, the auditor should document the risk factors and the response. Any additional factors and the responses noted during the audit should also be documented.

Whenever the auditor has determined that a fraud may exist, it should be brought to the attention of an appropriate level of management.

The effective date of SAS No. 82 is for periods ending on or after December 15, 1997.

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS
REPORT TO THE NATION

In 1995, the Association published and distributed their "Report to the Nation on Occupational Fraud and Abuse". Occupational fraud and abuse (employee fraud) is a serious problem in the United States. This report represents the largest known privately funded 2.5 year study on this subject. A total of 2,608 CFEs contributed details of actual fraud and abuse cases totaling $15 billion. The majority of these CFEs work for organizations where they are responsible for resolving allegations of occupational fraud from inception to disposition. Collectively, they have investigated more than 1 million cases of criminal and civil fraud. From this data, the report analyzes four areas: (1) the cost of occupational fraud and abuse; (2) the victims; (3) the perpetrators; and, (4) the methodologies.

The Association provided the following summary of the report:

(1) Fraud Facts.

- Employee theft occurs in 95% of American companies.
- Thirty-three percent of all employees have stolen money or merchandise on the job at least once.
- Fraud and abuse costs employers an average of $9 a day per employee. Organizations lose 6% of annual revenue to fraud. Small companies are more vulnerable.
- Fraud and abuse costs U.S. organizations more than $400 billion annually. There are no statistics for Oregon.
- Men commit three-fourths of fraud and abuse cases nationally. The typical perpetrator is a college-educated white male.
- Median losses caused by executives were 16 times those of their employees.
- Losses to perpetrators age 60 and older were 28 times those caused by perpetrators age 25 or younger. The largest losses can be found in the real estate financing industry, while the smallest are found in education.
- More checks are stolen than cash.
- Most fraud is detected as a result of complaints from other employees, not through audits.

(2) Prevention.

- Separate financial tasks so no one employee has total control.
- Conduct audits, either yearly or every few years depending on the size of the organization.
- Never sign a blank check.
- Involve customers by asking them to always ask for and get a receipt for payments. If they don't, tell them to report it.
- Prosecute suspected embezzlers.
- "The wrong approach to fraud prevention is accusing your employees of being thieves," said Joseph T. Wells, chairman of the Association of CFEs. "It can become a self-fulfilling prophecy. Instead, give employees a hotline, a place to report things they think are wrong."

Citizen Expectations

Plan For Success

The citizens of the State of Washington have two major expectations when they give their hard-earned money to any governmental entity. The government must:

- Safeguard the money while it is under their control.
- Spend the money wisely and for authorized purposes.

Therefore, governments must do everything possible to meet these public expectations. So, what should you do?

(1) Ensure that elected public officials, directors, and managers believe that internal controls are important. Auditors call this "Tone at the Top".

(2) Ensure the government establishes the proper separation of duties between key employees and managers to reduce the likelihood that one person would be able to completely control a process or function from beginning to end. **Two critical issues** associated with internal control are: (a) Don't tempt your employees; and (b) Don't put your employees at risk.

(3) Ensure that systems are put in place to monitor all revenue streams. This includes identifying all revenue sources/fees; determining where they enter the organization; including them in the budget (including analytical procedures to do so); and, monitoring budget versus actual to ensure that revenue matches your expectations.

(4) Ensure that systems are put in place to review all disbursements for propriety. Also ensure that someone independent of the bank account custodian reconciles the monthly bank statement promptly (within 30 days of statement date) and receives the bank statement directly from the bank unopened.

The degree to which you do these things affects your audit costs. You are in control of your

destiny. Good internal controls help to ensure a good audit (clean, with no findings) at less cost. If internal controls are weak and accounting records area a mess, you should prepare for the worst. Audit costs will undoubtedly increase, and fraud could even occur. A word to the wise should be sufficient.

Planning For Success in Fraud Cases

(1) Initial fraud detection by audit staff or notification of fraud by entity staff.

Telephone contacts, e-mail messages, or direct on-site meetings **(Critical Step)**

Entity staff should document a chronology document of events

Protection of accounting records from loss and notifications to key staff

Security of office, and employee's desk and computer

Employee interview, administrative leave or termination, and restitution agreement

Filing police report and notifying county prosecuting attorney's office

(2) Fraud development by audit staff.

Determining "what else" is at risk or universe of transactions **(Critical Step)**

Stay focused. This is where the battle for audit scope and costs is won or lost

Analytical procedures and scanning/testing of documents for other irregularities

Documenting internal control weaknesses that allowed the loss(es) to occur

Employee interview, administrative leave or termination, and restitution agreement

Determining lay-out of fraud information in audit working paper file **(Critical Step)**

Original source documents

Lead sheet summarizing fraud case by type of loss

Followed by fraud losses by individual type

FRAUD AUDIT PROGRAM

State agencies and local governments in the state of Washington are required to notify the State Auditor's Office when fraud is suspected or detected (RCW 43.09.185).

General Requirements:

- Notify the State Auditor's Office if you suspect or detect fraud or other irregularities.
- Protect the accounting records from destruction.
- Don't make a restitution agreement with the suspect prior to an audit to establish the amount of loss in the case. These agreements must be approved by the State Auditor's Office and the Attorney General's Office.
- Ensure that you take any personnel action based on the employee not following entity policies and procedures, not for misappropriating public funds (civil versus criminal).
- File a police report when advised to do so by the State Auditor's Office. Generally, this will be at the end of the investigation. We refer all fraud cases in government for prosecution.

TWO MAJOR TYPES OF RISK FOR FRAUD

- Cash Receipts.

  While the risk that fraud will occur in the cash receipts function is high, the dollar amount of losses from each case is usually small.

- Cash Disbursements.

  While the risk that fraud will occur in the cash disbursements function is low, the dollar amount of losses from each case is usually large.

STATE OF WASHINGTON State Auditor's Office	BULLETIN	No. 1999-03 Page: 1 of 2 Date: 11/05/99 Supercedes: 007

TO: **All Political Subdivisions**

FROM: **Brian Sonntag, CGFM**
State Auditor

SUBJECT: **Reporting Losses of Public Funds or Assets or Other Illegal Activity**

Revised Code of Washington (RCW) 43.09.185 requires that all state agencies and local governments **immediately** notify the State Auditor's Office (SAO) in the event of a known or suspected loss of public funds or assets or other illegal activity.

Entities are encouraged to develop policies and procedures to implement this statute. This guidance should establish an individual responsible for informing managers and employees about these reporting requirements and ensuring SAO is promptly informed of losses as required. These actions will also help to ensure that:

- Losses are minimized.
- Investigations and audits are not hampered.
- Improper settlements are not made with employees.
- Incorrect personnel actions are not taken.
- Employees are protected from false accusations.
- Bond claims are not jeopardized.

Entities should take the following actions when a loss of public funds or assets or other illegal activity is suspected or detected:

- Notify appropriate entity managers who are not involved in the loss. This may include the governing body, agency head or deputies, chief financial officer or internal auditor, depending upon the circumstances. Providing notification to your legal counsel may also be appropriate.
- Report the loss to the SAO Audit Manager in your area, or his/her designee.
- Protect the accounting records from loss or destruction. All original records related to the loss should be secured in a safe place, such as a vault, safe or other locked file cabinet, until SAO has completed an audit.

- Don't enter into a restitution agreement with an employee prior to an audit to establish

the amount of loss in the case.
- Ensure that any personnel action is taken based on the employee not following entity policies and procedures, rather than for misappropriating public funds (civil versus criminal).
- File a police report with the appropriate local or state law enforcement agency when advised to do so by SAO.

Entities should **immediately** notify the appropriate local or state law enforcement agency of the following:

- Suspected losses involving the health or safety of employees or property.
- Losses resulting from breaking and entering or other vandalism of property.

Entities **are not required** to report the following to 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 by cashier for any unusual trends.
- Reasonable inventory shortages identified during a physical count. Record inventory adjustments in the accounting system.
- Breaking and entering or other vandalism of property.

Please **do not** attempt to correct the loss without reporting to the authorities identified above. In addition, RCW 43.09.260 requires written approval of the State Auditor and Attorney General before state agencies and local governments make any restitution agreement, compromise, or settlement of loss claims covered by RCW 43.09.185.

If you have any questions about these procedures, please contact Joseph R. Dervaes, Audit Manager for Special Investigations, at (360) 710-1545 or by e-mail at dervaesj@sao.wa.gov.

Critical Actions Checklist for New Fraud Cases

State Agency or Local Government.

Revised Code of Washington (RCW) 43.09.185 requires that all state agencies and local governments **immediately** notify the State Auditor's Office (SAO) in the event of a known or suspected loss of public funds or assets or other illegal activity.

This critical actions checklist for new fraud cases follows the guidance contained in SAO Bulletin 1999-03, Reporting Losses of Public Funds or Assets or Other Illegal Activity. This information is designed to ensure that all fraud cases are properly managed. The audit team should advise the entity to do at least the following:

- Prepare a chronology document describing the events that led up to this report of loss. The staff's research and any information obtained in an interview with the employee believed responsible for the loss, such as an admission, should be included in this document. This document should be obtained and retained in the audit working paper file.

  The purpose of any interview would be to determine what was done, how the irregular transactions were recorded in the accounting system, how long the irregular activity occurred, and the estimated amount of the loss. The interview should be conducted in a conference room for privacy purposes with the door closed, but not locked. Advise the Entity how to set-up the room to ensure that a custodial situation (Miranda Warnings) was not created (i.e.; no one blocking the employee's exit from the room). If the employee is a member of a union bargaining unit, s/he is entitled to union representation (Weingarten Warnings) or to have another person of their choosing present during the interview. The entity must be prepared to put the employee on administrative leave (with or without pay, at its discretion), pending the outcome of the investigation/audit. This should be done immediately after the interview has been conducted. At the conclusion of the interview, the entity should obtain all office keys from the employee, cancel computer passwords and access, and change any safe/vault combinations if the employee had knowledge/access.

- Protect the applicable accounting records from loss or destruction. All original records related to the loss should be secured in a safe place, such as a vault, safe or other locked file cabinet, until the investigation/audit has been completed.

  The entity may not be able to access some records due to privacy issues associated with the employee's desk. Critical to this determination is whether the entity has a policy stating that the employee's desk is organizational or personal. If organizational, the organization must exercise its right to inspect the desk periodically. Otherwise, the desk reverts to personal. If personal, the entity must obtain a search warrant in order to access documents that were either in or on the desk. In these cases, the law enforcement agency must present sufficient facts to a judge demonstrating probable cause for this action. After an employee has been placed on administrative leave, the employee should be allowed to remove any personal items from the office and desk, under supervision, prior to departing the entity. After this has occurred, the entity will be able to access the employee's desk without any further

concern for privacy issues.

- Inform appropriate entity managers about the loss. This may include the governing body, legal counsel, agency head or deputies, chief financial officer or internal auditor, depending upon the circumstances. If the entity does not have a policy implementing RCW 43.09.185, this is a good time to remind managers about this important requirement. This helps to ensure that all future fraud reporting by the entity is properly handled.

- Refrain from entering into a restitution agreement with an employee prior to an investigation/audit to establish the amount of loss in the case.

  A draft restitution agreement that has been approved for use by SAO and the AGO is available from Team SI. Pursuant to RCW 43.09.260 (local governments) and RCW 43.09.310 (state agencies), a restitution agreement should not be finalized until SAO (Audit Manager for Special Investigations) and the applicable AGO representative have approved it. Notice of approval may be provided by telephone, e-mail, or letter, depending upon the circumstances of each case. The restitution agreement should include the amount of the loss and SAO audit costs. At the discretion of the entity, it may also include the organization's internal investigative costs. While the restitution agreement is approved by SAO and AGO, the actual agreement is a unilateral document between the entity and the employee and is signed only by these two parties.

- Ensure that any personnel action is taken based on the employee not following entity policies and procedures, rather than for misappropriating public funds. This separates the civil action from any future criminal action in the case. Obtain a copy of any such document for the audit working paper file.

- File a police report with the appropriate local or state law enforcement agency having jurisdiction. This notification may be made at the beginning of the case or may be deferred until the amount of the loss in the case has been determined.

  The purpose of the police report filing is to ensure that a police investigation is conducted in the case. This investigation is then referred to the appropriate county prosecuting attorney's office (39 such counties in the State of Washington). All recommendations for charges to be filed in the case come from the police investigation, not the organization's investigation or an audit. This is an important action. If a police report is not filed in the case, there never will be a prosecution in the case. An investigation report by the entity or an audit report by the State Auditor's Office, even if forwarded to the appropriate county prosecuting attorney's office, will not result in a prosecution. Such reports simply fall on deaf ears.

  The entity should also be prepared to make a press release with the details of the case once the police report has been filed. This document should indicate that the entity's internal controls detected the loss (if appropriate), that all agencies have been notified as required by state law, and that any internal control weaknesses that allowed this loss to occur and not be detected over a period of time have been corrected. The purpose of this document is to focus on the acts of the dishonest employee rather than on the entity, the victim in the case.

- Notify the (Name) County Prosecuting Attorney's Office having jurisdiction. This notification may be made at the beginning of the case or may be deferred until the amount of the loss in the case has been determined.

  SAO may make this notification on behalf of the entity. At the completion of each fraud audit, SAO initially sends a draft copy of the audit finding on the misappropriation to the County Prosecuting Attorney's Office. In the recommendations of each audit finding, we also refer all cases to the applicable County Prosecuting Attorney's Office for any further action deemed appropriate under the circumstances (i.e.; prosecution).

Washington State Auditor's Office.

One of the most important questions that must be answered on all new fraud cases is "what else" did the employee do to misappropriate public funds/assets from the entity, if anything.

The audit team should review the operational environment to determine the internal control weaknesses that allowed this loss to occur and go undetected for a period of time, if any.

- An inappropriate segregation of duties is the primary internal control weakness associated with any loss.

- All cases involve a compromise of the internal control structure, in one way or another, which allows the irregular transactions to be processed without detection by management over a period of time. Thus, a lack of monitoring procedures is usually a secondary cause.

- The entity must also be able to fix responsibility for funds to a particular person, at a particular point in time, all the time. The central question is: "Who's responsible for the money right now?" If this cannot be determined, our ability to determine the employee responsible for the loss is diminished. If this condition exists, the amount of audit resources devoted to the case may be restricted. We would then recommend the entity change its procedures to be able to fix responsibility for funds in the future.

Employees do what they have access to and can control. Therefore, the audit team should also use entity staff to help assess other areas for additional audit work other than the primary area noted in the preliminary loss report. These expanded audit tests can consume a significant amount of audit budget. We must always be aware of the cost effectiveness of the work performed (i.e.; audit costs in relation to the size of the detected loss). Therefore, care should be exercised when performing this work.

The audit team should use all available analytical procedures, such as by reviewing revenue or disbursement trends and by scanning documents and records in these additional areas, to identify areas where additional audit work is warranted. In these cases, only limited testing should be performed. If no further irregularities are noted from this work, the audit team should cease work in the area. The objective of this expanded work is to: (a) eliminate other areas from

further audit consideration; and, (b) to include all areas where fraud has been found. We should always stay focused here because this is where the battle over reasonable audit costs is won or lost.

STATE OF WASHINGTON FRAUD STATISTICS

January 1, 1987 through December 31, 2003

CALENDAR YEAR		NUMBER OF CASES		LOSS AMOUNTS	
1987\		32\		$ 388,936\	
1988 \	6 Year	26 \		451,122 \	
1989 \	Average	31 \	23	358,654 \	301,582
1990 /		15 /		120,121 /	
1991 /		15 /		264,027 /	
1992/		20/		226,629/	
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	
2000		30		167,363	
2001		68 **(Note)**		484,060	
2002		56		1,122,328	
2003		62		2,253,394	
17 Year Total		594		$12,215,222	
17 Year Average		35		$ 718,542	(Doubled +)

Note. The number of fraud cases doubled when RCW 43.09.185 was implemented. This statute requires all state agencies and local governments to immediately report known or suspected loss of public funds or assets or other illegal activity to the State Auditor's Office. As a result, many small cases of losses of funds that were not previously reported to us are now being tabulated in the annual fraud statistics.

Washington State Auditor's Office
Summary of Audit Reports Disclosing Fraud
January 1, 1996 through December 31, 2001

Description	CY2001	CY2000	CY1999	CY1998	CY1997	CY1996	Total	Percent
Cash Receipts								
Negative Cash Transactions (Fees/Adjustments)	2,541	4,929	17,651	9,060	337,783	37,460	409,424	8.5
Missing Bank Deposits	22,567	7,714					30,281	0.6
Cash Shortages	166,580	30,043	194,343	1,339	30,747	13,190	436,242	9.1
Money Laundering	772	13,662	1,728	200,374	189,523	484,011	890,070	18.6
Police Evidence Funds	1,750	17,709	9,263				28,722	0.6
Stolen Cash Receipts (Mysterious Disappearance)	8,840	4,893		5,700	15,036	120,656	155,125	3.2
Gross Profit Tests (Retail)		2,895		13,219	17,390		33,504	0.7
Check for Cash Substitution Scheme	3,125		213,669	6,448	50,793		274,035	5.7
Total Cash Receipts	206,175	81,845	436,654	236,140	641,272	655,317	2,257,403	47.1
Cash Disbursements								
Fictitious Petty Cash Transactions	4,289	2,344	4,814	1,386		4,707	17,540	0.4
Fictitious Claims & Travel Transactions	86,895	13,232	172,433	64,513	740,784	256,081	1,333,938	27.8
Issue Checks to Self or to Pay Personal Bills	69,183	40,669	157,235	218,520	44,007	7,746	537,360	11.2
Personal Purchases on Procurement/Credit Cards	31,424	1,499	553	2,887		835	37,198	0.8
Payroll Issues (Leave, Deductions & Hours of Work)	7,199	2,451	10,449	6,544	36,955	19,738	83,336	1.7
Personal Use of Telephone	43,030		1,056				44,086	0.9
Issuance of False Checks Drawn on Entity Account	28,162						28,162	0.6
Total Cash Disbursements	270,182	60,195	346,540	293,850	821746	289,107	2,081,620	43.4
Other								
Personal Use of Assets or Benefit	750	270				12,783	13,803	0.3
False Bus Ridership Records		22,603					22,603	0.5
Stolen Equipment and Supplies	6,687	2,450	87,550	67,489	58,456	800	223,432	4.7
Conflicts of Interest or Ethics Violations			5,800		18,894	798	25,492	0.5
Fictitious Medical Coverage			4,505				4,505	0.1
Theft of Trust Funds by Attorney			166,064				166,064	3.5
False Claims for Medical Benefits (Med IRA Acct)	266						266	0.0
Total Other	7,703	25,323	263,919	67,489	77,350	14,381	456,165	9.5
Total Fraud Losses	484,060	167,363	1,047,113	597,479	1,540,368	958,805	4,795,188	100.0
Total Fraud Cases	51	30	42	31	33	48	235	100.0
Average Fraud Loss Per Case	9,491	5,579	24,931	19,274	46,678	19,975	20,405	

Washington State Auditor's Office
Summary of Audit Reports Disclosing Fraud
January 1, 1996 through December 31, 2001

Description	CY 2001		CY 2000		CY 1999		CY 1998		CY 1997		CY 1996		Totals		%	%
	No.	Amount	No.	Amount	No.	Amount	No.	Amount	No.	Amount	No.	Amount	No.	Amount	No.	Amount
State Agencies																
State Boards and Commissions	4	110,546	1	270	1	144,422							6	255,238	2.4	5.3
Colleges and Universities	14	57,928	3	5,259	7	9,614	5	17,820	4	69,551	11	559,331	44	719,503	17.5	15.0
Department of Transportation	1	1,183	1	4,929			1	49,000	1	52,984			4	108,096	1.6	2.3
Department of Social & Health Services			1	2,450			1	9,652			2	5,499	4	17,601	1.6	0.4
Dept. of Comm. Trade & Economic Develop.			1	12,999									1	12,999	0.4	0.3
Secretary of States Office			1	25,420									1	25,420	0.4	0.5
Washington State Library			1	2,451									1	2,451	0.4	0.1
Department of Natural Resources					1	1,728					2	183,005	3	184,733	1.2	3.9
Department of Licensing	1	4,754			2	2,393	1	410					4	7,557	1.6	0.2
Department of Fish and Wildlife	1	14,892					1	137,467					2	152,359	0.8	3.2
Superintendent of Public Instruction							1	2,549					1	2,549	0.4	0.1
Attorney General's Office									1	8,610			1	8,610	0.4	0.2
Department of General Administration											1	2,705	1	2,705	0.4	0.1
Employment Security Department	2	81,391									1	2,901	3	84,292	1.2	1.8
Department of Corrections	2	4,427									1	0	3	4,427	1.2	0.1
Washington State School for the Blind	1	6,564											1	6,564	0.4	0.1
Total State Agencies	26	281,685	9	53,778	11	158,157	10	216,898	6	131,145	18	753,441	80	1,595,104	31.7	33.3
Local Governments																
Cities & Towns	7	32,425	5	54,537	10	206,900			6	614,339	7	21,534	35	929,735	13.9	19.4
Hospitals & Health Districts	4	3,080	2	4,492	5	291,047	3	15,481	2	2,214	2	7,214	18	323,528	7.1	6.7
Transit Authorities	1	253			1	166,064					2	667	4	166,984	1.6	3.5
Counties	5	56,532	6	14,644	4	159,946	4	19,506	1	5,472	4	31,608	24	287,708	9.5	6.0
School Districts & Educational Svc. Dists.	17	62,199	5	28,801	4	40,081	8	204,566	10	233,295	6	35,680	50	604,622	19.8	12.6
Housing Authorities					1	12,813	2	75,700			4	81,687	7	170,200	2.8	3.5
Public Utility Dists. & Water Districts	3	22,643	2	131	2	5,800	1	11,968	3	545,781			11	586,323	4.4	12.2
Ports					1	4,505	1	52,312					2	56,817	0.8	1.2
Miscellaneous Local Governments	3	7,500	1	10,980	3	1,800			1	1,257	2	14,623	10	36,160	4.0	0.8
Courts	2	17,743					2	1,048	4	6,865	3	12,351	11	38,007	4.4	0.8
Total Local Governments	42	202,375	21	113,585	31	888,956	21	380,581	27	1,409,223	30	205,364	172	3,200,084	68.3	66.7
Total Fraud Losses	68	484,060	30	167,363	42	1,047,113	31	597,479	33	1,540,368	48	958,805	252	4,795,188	100.0	100.0

FRAUD CASE ANALYSIS

Washington State Auditor's Office

	NUMBER OF CASES	PERCENT OF CASES
Trials	8	4
Plea Bargains	70	40
No Fixed Responsibility (File On Bond)	58	33
Case Not Prosecuted:		
Restitution Only	19\	11\
Other (Too Small, No Criminal	\	\
Intent, Unusual Case	= 41	= 23
Circumstances, Diversion)	16 /	9 /
Suspect Fled Prosecution	6 /	3 /
Total Closed Cases	177	100
Pending/Unresolved Cases	47	
Total Cases (1987-1995)	224	

THE AVERAGE FRAUD
Washington State Auditor's Office

The average fraud case in the state of Washington (1987-2001) is only $18,596.

The average fraud:

- Is discovered by management when properly following-up on exception transactions.
- Is detected by Assistant State Auditors while performing ordinary testing of original source documents during routine audits.
- Is a one-year event (or less).

FRAUD DETECTION INFORMATION

Internationally - 19%.

Internal and external auditors combined. (Source: Michael Comer, International Fraud Expert.)

State of Washington - 30%. (Source: State Auditor's Office statistical data base.)

Internal and external auditors combined (1987-2001).

- Demonstrates the effect of a strong fraud training program.
- Means we know our audit environment (state agencies and local governments).

The rest are found by management, whistleblowers, and taxpayers - 70%. Entity managers account for the majority of the frauds detected in the state of Washington.

- Fraud awareness seminars presented to state agency and local government managers as well as professional associations helps to improve both fraud prevention and detection.

TRIAL RECORD (1987-2001)
Washington State Auditor's Office

CASE YEAR	ENTITY	LOSS AMOUNT	TRIAL DISPOSITION GUILTY	TRIAL DISPOSITION NOT GUILTY
1987	Jefferson County	$ 1,607	XXX	
1987	Chelan County (No criminal intent was proved.)	974		XXX
1988	City of College Place (No criminal intent was proved.) (Recovery of funds by civil suit.)	1,585		XXX
1989	Lower Columbia College	139,130	XXX	
1991	Quillayute Valley School District (No criminal intent was proved.)	1,849		XXX
1992	Columbia Irrigation District	32,549	XXX	
1994	City of Longview	665	XXX	
1995	Olympic College (No fixed responsibility.)	4,018		XXX
1997	City of Battle Ground	49,895	XXX	
1998	Benton County	1,000	XXX	
1999	Seattle School District (SPICE Program)	180,913	XXX	
1999	Pike Place Market	173,875	XXX	
12	Total Court Cases	$ 414,185	8	4
===		=======	=	=

TOTAL COURT CASES:

- Less than one court case per year.
- Trial win-loss record is 67%-33%.

  Of the four trial losses:

  - Three involved no proof of criminal intent even though the crime actually occurred.
  - One involved no fixed responsibility for the loss which means that the internal control structure was compromised.

PRIMARY GOALS IN FRAUD DEVELOPMENT

- Control the scope of the audit
- Be 100% accurate
- Don't go to court (but always be ready)

CONCLUSIONS OF CASE STUDIES

- Need to get back to basics
- Most frauds employ common and simple methods
- Common sense is the most valuable resource
- Detection is everyone's job -- Development requires a specialist
- Awareness is the key to fraud detection

REASONS AUDITORS FAIL TO DETECT FRAUD

- Lack of or insufficient analytical procedures to detect fraud
- Lack of or insufficient detail testing **from** original source documents to accountability records
- Lacking an awareness of fraud indicators or the specific exposures of fraud
- Not recognizing basic internal control weaknesses which could lead to fraud
- "Mechanically" going through the audit process where form takes precedence over substance of audit work
- Don't want to find errors or fraud
- Accepting any client explanation for audit exceptions
- Audit budgets cause inadequate time to be spent on high risk areas

TYPES OF FRAUD

On-Book: Manipulated through the accounting records

Off-Book: Bribes, kickbacks, conflicts of interest

TYPES OF FRAUD PERPETRATORS

Active: Driven by motivation or greed

Don't hire this crook

Passive: Driven by temptation of weaknesses in internal controls

Honest person who changes into a dishonest person

Percentage of on-book passive frauds

Private sector: 70%

Government: 100% (almost)

FRAUD INTERACTION FACTORS

THEORY: Opportunity + Motivation = Fraud

Opportunity: Access/Skill/Time

This is every entity employee

Motivation: Justification/Challenge/Revenge/Financial Need

This is a very small percentage of all entity employees

REAL WORLD: Greed + Internal Control Weaknesses = Fraud

FRAUD PERPETRATOR CHARACTERISTICS

Washington State Auditor's Office

- The trusted employee or supervisor -- Your neighbor
- 50% Male -- 50% Female
- Has been employed for 3-5 years
- Changes over time (not the same today as when they were initially hired)
- Ignores or compromises established internal controls
- **Blind trust** is involved by the individual's supervisor
- Uses common and simple methods
- Basically unable to handle temptation -- Greed is often involved
- Unpredictable as to position and background
- No composite drawing

Managers (not auditors) must know when employees are experiencing a financial need (crisis) in their life.

When problems arise, management must consider the need for a temporary change in the duties and responsibilities of this employee.

If a change in duties and responsibilities is not practical, increased monitoring of activities of this employee is required.

CAUSES OF FRAUD

The root cause of fraud **outside** the organization is an individual's need for money, either real or perceived (greed). This financial need can arise from practically anything, including: catastrophic medical expenses, college and wedding costs for children, cost of nursing home care for parents, drugs and alcohol, gambling, supporting multiple family units, living beyond their means, excessive vacation and travel, credit card and other debt, lots of "toys" (i.e.; cars, boats, trailers, etc.). Supervisors must have sufficient knowledge about their employees to know when these conditions occur.

The need for money is just as great for those in positions of authority as it is for individuals at lower levels within the organization. Many people live one paycheck away from disaster. When a traumatic event such as the loss of a job by a spouse or down-sizing/right-sizing within the organization impacts a member of the family unit, everything financial begins to collapse immediately. **Everyone can do something** within the organization to create fraud. They simply do what they have access to and what they can control. Therefore, an honest person changes to a dishonest person overnight. They then come to work one day and begin to commit fraud.

The root cause of fraud **inside** the organization is an inadequate segregation of duties. This is where one individual has total control over a transaction from beginning to end. When it's not possible to segregate duties between two or more employees, establish a monitoring program for this key employee which effectively accomplishes a segregation of duties without hiring another individual to perform the task.

Employees capitalize on a weakness in internal controls or the lack of monitoring of what they do by management. Relatively common and simple methods are used to commit fraud. It's the concealment of the activity that often makes these cases complex.

Eventually, these employees will make a mistake. Therefore, proper follow-up on exceptions noted during routine business activity is essential to detect fraud. All mistakes are not fraud; but, some are. Where there's fraud, there's smoke. Don't be too quick to accept the first plausible explanation for deviations from normal procedures. Find out if it's the right answer to the problem.

Of course, a strong internal control structure that is monitored by management officials is an effective deterrent mechanism in the fight against fraud. Employees who commit fraud simply ignore or compromise internal controls to do what they need to do. They simply don't play by the rules. Managers must promptly identify when employees do not use the organization's procedures to detect fraud early and keep any resulting losses to a minimum. In addition, a strong internal control structure increases the likelihood that management can fix responsibility for misappropriations of public funds, thus protecting innocent employees from suspicion or false accusations.

Some internal controls are for the organization, some are for the employee, and some are for both the organization and the employee. The first response to new internal controls is: "Don't you trust me?". This can easily be resolved by emphasizing that the entity is a steward of the public's money and that taxpayers hold the government accountable to use their funds wisely and to protect them from loss while in their custody.

Fraud can never be eliminated entirely. So, it's always going to be with us.

CONSISTENT PATTERNS IN FRAUD CASES

- Frauds tend to be progressive
- Some type of an "accounting problem" is the first defense
- Perpetrator will admit to what the auditor knows
- Perpetrators are unpredictable as to position and background
- The number one internal control weakness is "**blind trust"**
- Most frauds are passive and on-book (70%)
- There is a high rate of repeat offenders
- There is no relationship between the loss amount and the skills needed to commit the fraud
- Many frauds go undetected
- A fraud specialist needs to be on-site
- Interviews are the most critical step of a fraud audit
- It's impossible to satisfy everyone
- Early audit involvement is needed
- The real cost of fraud goes beyond the monetary loss
- Trials are a no win situation
- You can't depend on internal controls to be observed
- Data processing frauds are no different than manual frauds
- Management doesn't believe it will ever happen again
- Fidelity bonds are a poor protection against fraud losses
- Perpetrators change over time (the "chameleon" effect)
- Perpetrators very rarely save what they take -- they spend it
- Perpetrators act out of character by performing tasks they shouldn't

THE SYSTEM OF INTERNAL CONTROL

Internal control structure responsibilities are as follows:

Management: Establish and monitor internal controls.

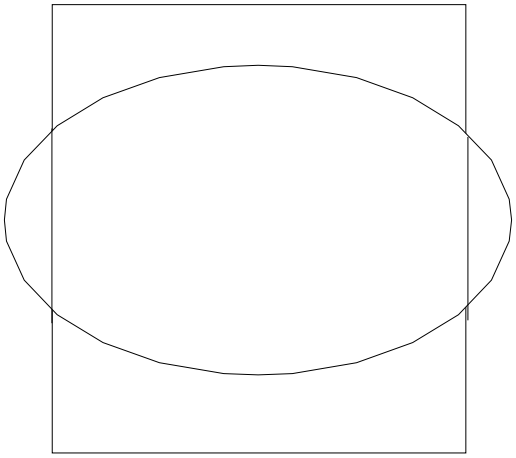
Audit: Evaluate and test internal controls.

What fraud perpetrators do -- **They simply don't play by the rules**. They do the following:

- Ignore internal controls established by management.
- Compromise internal controls established by management.

There are two categories of fraud perpetrators: doers (first line employees) and reviewers (supervisors).

The circle/square concept (Example):



- The "circle" represents the internal control procedure involved, such as making organization bank deposits on a daily basis.
- The "square" represents what the employees really do when they perform their jobs. All fraud cases represent squares. The amount of loss is based upon how quickly managers determine that the condition exists. But, when employees simply don't perform tasks as expected, this same condition exists, such as by making bank deposits on Monday, Wednesday, and Friday instead of each business day. Once these deviations from expectations are detected, it's important to get employees back on track quickly. Remember that people respect what you inspect, not what you expect. Therefore, monitoring of employee actions is a critical management function.

Major Problems:

Employees are tempted and even put at risk in work environments where internal controls are weak or not properly monitored to ensure that management's expectations are being met. Managers tell their employees what to do, expect them to do it, but then don't subsequently review their work once the job is done. This is called "blind trust", and is at the heart of many fraud cases. This condition causes two of our most significant problems.

(1) Lack of monitoring of employee tasks by managers is the first problem.

Managers expect supervisors to review the work of their subordinates. And, the vast majority of internal control procedures involve this relationship. But, usually no one reviews the work of the supervisor in the same way they monitor the work of their subordinates. As a result, this supervisor becomes the highest risk employee within the organization who could perpetrate a fraud and conceal it for a long period of time without detection by managers. The largest fraud cases in the past, right now, and in the future involve this supervisor.

Problem: The highest risk employee in your organization is the last person who prepares the deposit before it goes to the bank. And, that employee is a supervisor who occupies a critical position of trust within the organization. This allows the employee the opportunity to manipulate the contents of the bank deposit without detection, usually for long periods of time and resulting in huge dollar losses. This person operates at decentralized or departmental locations and at the central treasury function.

Solutions: An individual who is independent of the function involved must periodically verify the work of this key, trusted employee. Omitting this critical "last look" has been responsible for some of the largest cash receipting fraud cases in the state. If you're not doing this now, your procedures need to be changed immediately to ensure that the organization's resources are properly safeguarded from loss.

But how does an organization actually do this? Of course, the objective of your work is to perform an unannounced cash count to verify that the mode of payment of the cash receipting records for all transactions matches the check and cash composition of the daily bank deposit. There are several ways to do this. For example:

- Visit the supervisor's office location on a periodic and unannounced basis after the bank deposit has been prepared. Complete the verification identified above and then independently make the bank deposit.

- Make arrangements with your bank and have the bank deposit returned to the organization (unopened). The bank could return the bank deposit to an independent party at a designated location, or the organization could pick-up the bank deposit at the bank. Either procedure will work. Complete the verification identified above and then make the bank deposit.

- Make arrangements with your bank to process the daily bank deposit normally, but make copies the deposit slip as well as the checks and any other documents included in the deposit for the organization. These records should then be used to complete the verification identified above.

(2) Lack of fixed responsibility for funds is the second problem.

Problem: When, not if, losses occur, managers are unable to fix responsibility for losses to a specific employee. Employees are often accused unjustly under these circumstances. The number of cash receipting fraud cases in the state of washing with no fixed responsibility for the loss is way too high, and demonstrates that too many managers incorrectly deal with this risk today.

Solutions: Establish procedures to safeguard funds at all times. In during daily cashiering operations, each cashier should have their own change fund and password for computer cash register systems. Each employee who stores funds in a safe or vault overnight must also have a separate locking container. These procedures ensure the organization can fix responsibility for money to a particular employee, at a particular point in time, all the time. If you can't do this right now, your cash handling procedures need to be changed immediately to ensure that you properly protect your employees. The ultimate question is: "Who's responsible for the money right now?"

KEY INTERNAL CONTROL ISSUES FOR MANAGEMENT (AND AUDITORS)

There are five key internal control issues facing management (and auditors). These factors work interchangeably to define the entity's exposure to waste, theft or abuse of public assets.

- **EXPECTATIONS.** What are management's expectations with respect to financial operations? Examples include establishing budgetary revenue expectations for specific revenue streams (e.g. fundraisers, food services and student store operations, etc) and monitoring to actual levels. For example, ensuring food services revenues are consistent with the number of meals served (i.e. tray counts) and the number of free and reduced-priced meals reported to the Office of Superintendent of Public Instruction. As an illustration, if there were 1,000 meals served at a particular elementary school at the full rate at $1.50 each and 300 meals at the reduced rate of $.40 each, then revenues should be $1,620. Further, all claims for free and reduced-priced lunches should be properly authorized and supported. *Exceptions should be resolved in a timely manner*.

- **ACCOUNTABILITY.** How is accountability for assets established? Examples include usage and monitoring of official pre-numbered documents (e.g. receipts, lunch tickets, etc).

- **FIXED RESPONSIBILITY.** How is responsibility for assets established? The central method for addressing this is through controlling access to assets. Examples include usage of separate cash drawers, placement of imprest funds and revenues in a secure location (e.g. safe), etc. Also, are combinations to the safe written down? (this usually destroys the ability to effectively fix responsibility for losses).

- **UNIVERSE OF ACTIVITY**. How does management know that all activity for a given area has been identified and captured by the accounting system? Examples include ensuring all lunch tickets and meal cards have been identified, moneys due receipted and deposited intact, and food services inventory properly accounted for. The key is formal policies and procedures outlining monitoring requirements between the operations side (e.g. schools) and the accounting side (e.g. finance) of a given operation.

- **MONITORING.** How does management know whether organizational policies and procedures are being followed? Examples include ensuring official pre-numbered receipts are both used and accounted for in a timely manner. This is absolutely critical since, absent effective monitoring, the other four objectives lose their effectiveness.

EMERGING FRAUD TRENDS

(1) Documents which serve the same purpose as blank checks.

THE FRAUD:

Unauthorized transactions are processed on:

- Petty cash documents
- Travel vouchers
- Time cards/sheets/lists

All fraud occurs **after** approval.

Unused lines on these forms are then completed (falsified/altered).

PREVENTION:

Eliminate the use of blank lines on these forms (crossed-out).

All such documents should proceed directly to payment after approval and not returned to the source where they are revised/changed/forged.

Look for a **straight line** from source to approval to payment.

(2) Documents which eliminate the accountability for cash receipts in manual or computer systems (cash registers).

THE FRAUD:

Unauthorized transactions are processed for:

- Voids
- Paid-outs
- Refunds
- Non-cash credits
- Cancellations
- Adjustments

For every use of these transaction types, there is also an abuse.

PREVENTION:

Supervisory approval is required for these transaction types.

Use specific forms for these purposes.

Retain all copies of supporting documents on file.

Prepare exception reports for these transaction types.

Monitor the activity of these high risk transactions.

(3) Transmittals of funds from one location to another (i.e.; from decentralized location to central treasurer, and from central treasurer to bank).

THE FRAUD:

Mysterious disappearance thefts by unknown party.

Change funds/cash transmittals/bank deposits.

May conceal a lapping scheme because these losses eliminate the accountability for cash (which may have been misappropriated rather than stolen).

PREVENTION:

Prepare daily activity reports at decentralized locations.

Use prenumbered/controlled cash transmittal forms.

Use locking or tamper proof bank bags for transmittals to the central treasurer. Direct deposit to the bank is a better system, if practical.

Require two people to count funds at the central treasurer. This is a critical step, yet it is often overlooked.

Use locking or tamper proof bank bags for transmittals to the bank.

Use bank night depository facilities (or obtain a receipt).

(4) Negotiable instruments being stolen and redeemed without the knowledge or approval of the entity.

THE FRAUD:

Thefts of checks and warrants from storage locations (by both employees and outsiders). These negotiable instruments are then cashed.

PREVENTION:

Store both checks and warrants in locked storage facilities.

Limit the number of employees with access to storage facilities.

Monitor inventory of check and warrant stocks.

Maintain logs for negotiable instruments issued.

Promptly note sequence breaks from one run to the next.

Act immediately when numbers are missing (stop payment action).

Determine whether an investigation is needed (police report).

(5) Missing revenue streams.

THE FRAUD:

Employees collect the money and steal it.

All (or practically all) of the revenue from a particular source, usually at a decentralized operating location, is stolen.

Cash is stolen outright.

Checks must first be negotiated before funds can be used.

- ☞ Check for cash substitution scheme.
- ☞ Checks are laundered through entity bank accounts of all types and personal bank and credit union accounts.

PREVENTION:

Know your operation well.

Identify all known sources of revenues.

Ensure all sources of revenue are included in the annual budget.

Analyze financial reports and obtain valid explanations for budget to actual revenue variances.

Periodically review the composition of daily bank deposits.

Subpoena employee bank accounts and analyze bank deposits for irregularities, if appropriate.

Review the fund level of entity bank accounts, but concentrate on the activity/transactions being processed.

Control high risk checks by having two people open the mail, make a log or record of the transactions, and reconcile to cash receipts and bank deposits.

DANGER:

Analytical review procedures will detect a drop in reported revenue, but will not necessarily detect the absence of revenue from a particular source, or the theft of a constant amount or percentage of these revenues.

(6) Employees will steal checks.

THE FRAUD:

Contrary to popular belief, employees will steal checks from both revenue systems and disbursements systems.

- Checks must first be negotiated before funds can be used.
- Check for cash substitution scheme.
- Checks are laundered through entity bank accounts of all types and personal bank and credit union accounts.

PREVENTION:

Identify and eliminate all off-line accounts receivable systems because the outstanding balances, when collected, represent "free" money.

Identify and eliminate weaknesses in disbursement systems, both payroll and accounts payable, where employees have responsibilities for both input of transactions and output of checks (the "kiss of death" in fraud cases).

Refer to emerging trend (5) for additional fraud prevention steps.

(7) The payroll department is a cash receipting function.

THE FRAUD:

Payroll department employees collect funds from ex-employees who are allowed to continue their health/medical benefits in force by personally paying for the cost of this insurance coverage until they obtain other employment and coverage (COBRA Program).

Ex-employee payment checks are processed two ways:

- ☞ Checks are made payable to the entity, deposited, and the amount included in the entity's payment to the insurance carrier.

- ☞ Checks are made payable to the insurance carrier, but processed through the payroll department and consolidated with the entity's payment.

Health benefits are continued in force for ineligible people.

PREVENTION:

Reconcile suspense funds established to process these payments (agency fund using the zero balance concept).

Establish computer edits or manual controls to ensure that no one remains on the program longer than allowed.

Establish procedures to ensure that all participants are authorized and have been approved for the program by management.

DANGER:

Few people realize that money flows through the payroll department.

(8) All funds and accounts called "imprest/trust/suspense/dormant" are high risk and vulnerable to manipulation.

THE FRAUD:

Employees launder irregular transactions through these funds and accounts.

These funds and accounts are commonly used to conceal fraudulent activities anywhere within the entity. But, this is definitely a vulnerability in the treasury function.

PREVENTION:

Review the fund level of entity bank accounts, but concentrate on the activity/transactions being processed.

Someone independent of the fund or account custodian should reconcile the bank account monthly.

Restrict access to these high risk funds and accounts.

Require dual authorization/approval of all disbursements from these funds and accounts.

Prepare exception reports for these high risk transactions.

FOUR TROUBLESOME INTERNAL CONTROL AREAS FOR FRAUD

(1) Segregation of Duties:

Problem: One individual has total control over a transaction type from beginning to end.

Solution: When it's not possible to segregate duties between two or more employees, establish a monitoring program for this key employee which effectively accomplishes a segregation of duties without hiring another individual to perform the task.

(2) Check for Cash Substitution Scheme:

Problem: Unrecorded revenue checks (no cash receipt issued) are substituted for cash from transactions which were receipted and then laundered through the entity bank deposit. Accounts receivable systems are often involved.

Solution: Agree total cash receipts by mode of payment from the accounting records to a **bank-validated** deposit slip which lists the check and cash composition of the actual deposit.

(3) Checking Accounts:

Problem: Money laundering activities. Unrecorded revenue is deposited into checking accounts. Custodians then write checks to "cash", themselves, a bank (to purchase a cashiers check or money order), or to a fictitious vendor.

Solution: Someone **independent** of the custodian of any bank account or general disbursement system must perform the monthly bank reconciliation and review all canceled/redeemed checks for any irregularity. This person should receive the bank statement directly from the bank unopened.

(4) Collect the Money and Steal it:

Problem: Cashiers often work alone, particularly at decentralized locations (checks which arrive in the mail are the highest risk because they are often laundered through bank accounts of all types both internally and externally).). As a result, "skimming" (i.e.; misappropriating funds collected without creating accountability for the money) represents the primary **undetected** fraud that occurs every day.

Solution: Two individuals should open the mail, make a log or record of the transactions, turn these checks over to the cashier function, and then reconcile the log to daily cash receipts and the bank deposit to ensure that all transactions have been properly accounted for and controlled. An alternative solution is to use a bank lock box for large revenue streams.

METHODS USED TO LAUNDER ENTITY REVENUE AND DISBURSEMENT CHECKS

FACT: There are more people in the United States and in the State of Washington today who steal checks than ever before. Check fraud is a $16 billion industry annually, and growing.

Problem: Part of the problem is that many managers do not understand the risk associated with checks, and this needs to change. Employees steal **unrecorded** revenue checks and launder them both inside and outside the organization to receive the proceeds. The "laundering" is what the employees do to convert the checks for their own personal gain. Usually, the employees who steal these checks are not the ones that received them first. This means that the funds were received at one location and then transmitted to another location where accountability is supposed to be established. But, formal cash receipting of these transactions never occurs when employees steal the checks. During the five-year period 1996-2001, losses from money laundering fraud cases were $890,070 (18.6% of all dollar losses).

Solution: Since you can't control what happens outside the organization, managers must "capture" accountability for incoming revenue checks immediately upon receipt by recording the transactions on whatever receipting mechanism is used (i.e.; manual receipts, computer receipts, cash registers, etc.).

Ideally, two individuals should open the mail, make a log or record of the transactions, turn these checks over to the cashier function, and then reconcile the log to daily cash receipts and the bank deposit to ensure that all transactions have been properly accounted for and controlled. Few managers correctly deal with this risk today.

Governments should also restrictively endorse all checks "For deposit Only" immediately upon receipt.

In addition, someone independent of the custodian of any bank account or general disbursement system must perform the monthly bank reconciliation promptly and review all canceled/redeemed checks for any irregularity. This person should receive the bank statement directly from the bank unopened.

Perpetrators launder negotiable instruments **inside** the organization by:

(1) Using a check for cash substitution scheme in the organization's daily bank deposit.

(2) Making irregular deposits into and subsequent withdrawals from an authorized bank account with a name similar to the name of the organization, such as an employee fund.

(3) Making irregular deposits into and subsequent withdrawals from an authorized bank account used within the organization (i.e.; general depository, imprest, trust, etc.).

(4) Making a "cash-back" withdrawal from a deposit for any type of bank account at the organization.

(5) Altering checks by increasing the amount and removing an equivalent amount of currency from the till drawer and subsequent daily bank deposit.

Perpetrators launder negotiable instruments **outside** the organization by:

(1) Making deposits into a "bogus" bank account in the name of the organization.

(2) Making deposits into their own personal bank or credit union account.

(3) Cashing the checks at a financial institution or business/vendor.

TWENTY DANGER SIGNS OF EMBEZZLEMENT

1. Borrowing small amounts from fellow employees.

2 Placing personal checks in change funds (undated, postdated) or requesting others to "hold" check.

3. Personal checks cashed and returned for irregular reasons.

4. Collectors or creditors appearing at the place of business, and excessive use of telephone to "stall off" creditors.

5. Placing unauthorized IOUs in change funds, or prevailing on others in authority to accept IOUs for small, short-term loans.

6. Inclination toward covering up inefficiencies or "plugging" figures.

7. Pronounced criticism of others, endeavoring to divert suspension.

8. Replying to questions with unreasonable explanations.

9. Gambling in any form beyond ability to stand the loss.

10. Excessive drinking and night-clubbing, or associating with questionable characters.

11. Buying or otherwise acquiring through "business" channels expensive automobiles and extravagant household furnishings.

12. Explaining a higher standard of living as money left from an estate.

13. Getting annoyed at reasonable questioning.

14. Refusing to leave custody of records during the day or working overtime regularly.

15. Refusing to take vacations and shunning promotions for fear of detection.

16. Constant association with, and entertainment by, a member of a supplier's staff.

17. Carrying an unusually large bank balance, or heavy buying of securities.

18. Extended illness of self or family, usually without a plan of debt liquidation.

19. Bragging about exploits and/or carrying unusual amounts of money.

20. Rewriting records under the guise of neatness in presentation.

FORTY COMMON FORMS OF FRAUD

1. Pilfering postage stamps.
2. Stealing merchandise, tools, supplies, and other items of equipment.
3. Removing small amounts from cash funds and registers.
4. Failing to record sales of merchandise and pocketing the cash.
5. Creating overages in cash funds and registers by under-recording.
6. Overloading expense accounts or diverting advances to personal use.
7. Lapping collections on customer' accounts.
8. Pocketing payments on customers' accounts, issuing receipts on scraps of paper or in self-designed receipt books.
9. Collecting an account, pocketing the money, and charging it off; collecting charged-off accounts and not reporting.
10. Charging customers' accounts with cash stolen.
11. Issuing credit for false customer claims and returns.
12. Failing to make bank deposits daily or depositing only part of the money.
13. Altering dates on deposit slips to cover stealing.
14. Making round sum deposits and attempting to catch-up by the end of the month.
15. Carrying fictitious extra help on payrolls or increasing rates or hours.
16. Carrying employees on payroll beyond actual severance dates.
17. Falsifying additions on payrolls.
18. Destroying, altering, or voiding cash sales tickets and pocketing the cash.
19. Withholding cash sales receipts by using false charge accounts.
20. Recording unwarranted cash discounts.
21. Increasing amounts of petty cash vouchers and/or totals in accounting for disbursements.

22. Using personal expenditure receipts to support false paid-out items.

23. Using copies of previously used original vouchers or using a properly approved voucher of the prior year by changing the date.

24. Paying false invoices, either self-prepared or through collusion with suppliers.

25. Increasing amounts of suppliers' invoices through collusion.

26. Charging personal purchases to the employer through misuse of purchase orders.

27. Billing stolen merchandise to fictitious accounts.

28. Shipping stolen merchandise to an employee's or relative's home.

29. Falsifying inventories to cover thefts or delinquencies.

30. Seizing checks payable to the employer or to suppliers.

31. Raising canceled bank checks to agree with fictitious entries.

32. Inserting fictitious ledger sheets.

33. Causing erroneous footings of cash receipts and disbursement books.

34. Deliberately confusing postings to control and detail accounts.

35. Selling waste and scrap materials and pocketing proceeds.

36. "Selling" door keys or the combination to safes and vaults.

37. Creating credit balances on ledgers and converting to cash.

38. Falsifying bills of lading and splitting with the carrier.

39. Obtaining blank checks (unprotected) and forging the signature.

40. Permitting special prices or privileges to customers, or granting business to favored suppliers, for "kickbacks".

Twenty-Five (25) Life Rules

1. Some internal controls are for people, some are for the organization, and some are for both.

2. Employees ignore or compromise internal controls when fraud is committed. They just don't play by the rules.

3. No one employee should have total control over a transaction type from beginning to end. When it's not possible to segregate duties between two or more employees, establish a monitoring program to review the activities of this key employee.

4. Fraud is a many splendored thing. Anything can happen anywhere and at any time. Stay alert.

5. Don't tempt employees and don't put them at risk by having a poor internal control environment. Remember, the internal control structure self-destructs on breaks and at lunch.

6. Opportunity (i.e.; access, skill, and time) plus motivation (i.e.; financial need, justification, challenge, and revenge) equals fraud. Know your employees and what is happening in their lives.

7. There are two types of dishonest employees: "doers" (i.e.; first line employees) and supervisors. Not many people monitor the work of supervisors, and this is a greater risk because most internal controls are designed for the "doers".

8. Encourage employees to take at least one long vacation per year, and perform the employee's job while they're absent from the workplace.

9. Monitor, monitor, monitor. Everyone has the ability to do something, usually what they have access to and can control so that irregular transactions can be concealed.

10. Don't fall into the "blind trust" activity trap. Trust, but verify.

11. Fix responsibility for money to a particular person, at a particular point in time, all the time. Who's responsible right now?

12. There should always be one cashier, one change fund, and one person accountable for money.

13. Restrictively endorse all checks "For Deposit Only" immediately upon receipt.

14. Protect safe combinations and computer passwords. Limit access, change them frequently, delete when employees terminate employment, and don't write them down.

15. Know your revenue streams and "capture" accountability (i.e.; receipt either manually, by cash register, or by computer) for all revenue transactions immediately when and where it enters the entity. What are your expectations?

16. Use an exception report for all types of negative-cash credit transactions (i.e.; voids, refunds, paid-outs, non-cash credits in courts and for college scholarships, and cancellations, adjustments, and account write-offs in accounts receivable systems). Think about the universe of all transactions.

17. Two people should open the mail, make a log or record of the transactions, turn these checks over to the cashier functions, and then reconcile the log to daily cash receipts and the bank deposit to ensure that all revenue transactions have been properly accounted for and controlled.

18. "Skimming" entity revenue involves both currency and checks.

19. Money laundering stolen entity revenue checks is a major threat. People steal checks more often than currency.

20. Compare the mode of payment of cash receipts with the check and cash composition of the daily bank deposit. Check for cash substitution account for 25% of total fraud losses in this state.

21. Make bank deposits daily and intact.

22. Look for a straight line from source to approval to payment for petty cash documents, travel vouchers, and time and attendance documents. All fraud is after approval.

23. Have an independent party promptly (immediately) reconcile the bank account each month. This person should receive the bank statement directly from the bank, unopened.

24. Notify the State Auditor's Office about all known or suspected losses.

25. Don't enter into a restitution agreement with a suspect prior to an audit to establish the amount of loss in the case.

SUMMARY

- Fraud causes the public to lose faith and trust in government.

- Fraud causes unwanted media coverage (usually front page because of increased interest). This event also has the potential to be politically embarrassing to the government, particularly after internal control weaknesses have previously been the subject of audit reports.

- The best defense against fraud is a good offense (for both deterrence and detection purposes). This is where an ounce of prevention is better than a pound of cure.

- The challenge is to go back to work and monitor something (anything).

- Awareness that fraud can (and does) happen is the key to detection.

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

General Fraud Information

Definitions
Fraud Detection Methods - General
Fraud Detection Methods - Cash Receipts
Fraud Detection Methods - Cash Disbursements
Collusion
Segregation of Duties
The Trusted Employee
Brief Checklist to Identify “At Risk” Employees
Fraud/High Risk Decision Process (Auditor Mind Set)
A Suggested Internal Control Guide for Management Officials

DEFINITIONS

Webster's Dictionary (Fraud)

A deception deliberately practiced in order to secure unfair or unlawful gain. A piece of trickery. One who defrauds. Cheat. One who assumes a false pose. Imposter.

Black's Law Dictionary (Fraud)

An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury. Any kind of artifice employed by one person to deceive another.

A generic term, embracing all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated. (**This is the definition used by the Association of Certified Fraud Examiners**.)

Bad faith and fraud are synonymous, and also synonyms of dishonesty, infidelity, faithlessness, perfidy, unfairness, etc.

Elements of a cause of action for fraud include **false representation** (intentional and reckless) of a present or past fact (material point) made by defendant, action in reliance thereupon by plaintiff (**believed**), and **damage** resulting to plaintiff from such misrepresentation.

It consists of some deceitful practice or willful device, resorted to with intent to deprive another of his right, or in some manner to do him an injury. As distinguished from negligence, it is always positive, intentional. It comprises all acts, omissions, and concealments involving a breach of a legal or equitable duty and resulting in damage to another. And includes anything calculated to deceive, whether it be a single act or combination of circumstances, whether the suppression of truth or the suggestion of what is false, whether it be by direct falsehood or by innuendo, by speech or by silence, by word of mouth, or by look or gesture. Fraud, as applied to contracts, is the cause of an error bearing on a material part of the contract, created or continued by artifice, with design to obtain some unjust advantage to the one party, or to cause an inconvenience or loss to the other.

Revised Code of Washington (RCW)

RCW 9A.56.020 (Theft). Theft means: (a) to wrongfully obtain or exert unauthorized control over the property or services of another or the value thereof, with intent to deprive him of such property or services; or (b) by color or aid of deception to obtain control over the property or services of another of the value thereof, with intent to deprive him of such property or services;

or (c) to appropriate lost or misdelivered property or services of another, or the value thereof, with intent to deprive him of such properly or services.

RCW 9A.60.20 (Forgery). A person is guilty of forgery if, with intent to injure or defraud: (a) he falsely makes, completes, or alters a written instrument or; (b) he possesses, utters, offers, disposes of, or puts off as true a written instrument which he knows to be forged.

Other Definitions

> Embezzlement. Fraudulent appropriation of property by a person to whom it has been entrusted, or to whose hands it has lawfully come. It implies a breach of trust or fiduciary responsibility.
>
> Larceny. Wrongful taking and carrying away of the personal property of another with intent to convert it to one's own use or to deprive the owner of its use and possession.

The major distinction between embezzlement and larceny lies in the issue of the legality of custody over the article stolen. In embezzlement, the thief is legally authorized by the owner to take or receive the article and to possess it for a time. In larceny, the thief does not need to have legal custody. He feloniously takes the article from the owner. The formulation of intent to steal the article may occur subsequent to the time when it came into his possession or concurrently with initial possession. If intent to steal occurs subsequent to initial possession, the crime is embezzlement. If initial possession and intent to steal occur simultaneously, the crime is larceny.

Ways to Prove Intent

- Alteration of documents
- Concealment of evidence
- Destruction of evidence
- False exculpatories (lies)
- Personal gain
- Obstruction of justice
- Pattern of conduct (repetition)
- Testimony of co-conspirator
- Admissions
- Confessions

Burden of Proof

In **criminal** cases, the burden of proof is "beyond a reasonable doubt". Juries must rule unanimously on guilt.

In **civil** litigation, the standard of proof is much lower, and may be decided by merely a "preponderance of the evidence". The verdict also does not necessarily have to be unanimous.

FRAUD DETECTION METHODS - GENERAL

Approach each audit engagement cautiously by exercising due care and a high degree of professional skepticism.

Assess tone at the top of the organization (i.e.; “Who’s minding the store?”, and “Does anyone care?”).

Identify major organizational internal control weaknesses and significant functional areas of high risk for fraud. Review these internal controls carefully, and don’t overlook the obvious. Develop audit tests specifically designed to address the identified fraud risks.

Provide cyclical audit coverage of the significant functional areas of high risk for fraud. Perform an unannounced cash count at each function, remembering that this is the auditor’s one opportunity to see the square in action.

Review the segregation of duties of key employees in critical functions within the organization, and select areas for review based upon any weaknesses found.

Perform audit tests correctly (i.e.; not backwards), and at the original source document level (rather than at some summary level of activity). Audit tests are easy to perform at summary level where documents always balance and reconcile; but, frauds are detected only at source document level.

Don’t accept the first plausible explanation given by management for any exception detected during substantive audit testing. Perform a sufficient amount of follow-up audit work to ensure an understanding of all explanations given by management, including additional substantive audit tests when required. Always remember that the individual giving you the answer may be the fraud perpetrator (a person in a position of trust). The proper audit response to explanations given by management is: “Show me a transaction which when processed correctly will create this condition.” When routine processing errors are involved, managers will be able to provide adequate explanations. When fraud is involved, no one will be able to provide a valid explanation for the condition.

FRAUD DETECTION METHODS - CASH RECEIPTS

Perform a comparative analysis of revenues from one period to another for each local revenue source or function. Analyze significant fluctuations (up and down), and select areas for further review accordingly.

Prove the reliability of cash receipts by using alternative record verifications (i.e.; counters on machines, reasonableness testing of retail sales activities, and manual or mechanical counting of units used to measure revenue).

Perform an unannounced cash count, including a review of the check and cash composition on the date of the count as well as during substantive audit tests of cash receipts.

Perform a review of the sequential issue and use of official prenumbered documents and cash register "Z" tapes.

Perform a review of procedures for all void and non-cash credit transactions, including proper accountability for all supporting documents for these transactions.

Use covert surveillance techniques (i.e.; video cameras or other filming operations), when warranted.

Use periodic observations of facilities and employees, both overt and covert.

When properly analyzed, most computer fraud is really computer assisted fraud. There is nothing special about these fraud schemes because fraud perpetrators commit computer frauds and manual frauds exactly the same way. These frauds can also be observed and detected in the entity in other ways (traditional substantive audit tests).

Be inquisitive and alert at all times, and thoroughly understand the operating environment.

- A key question to ask is: "If I were a crook, how would I get the money (asset) out of here?" Once that's understood, that's probably how it's being done by entity employees (if at all).

- Another key question to ask, once a fraud has been detected, is: "What else does this person do?" If an individual is responsible for multiple functions, and fraud is detected in one of those functions, it's also likely that fraud will be detected in one or more of these additional functions as well.

Beware when the fund custodian resists your inquiries, both during interviews and substantive audit tests (i.e.; don't have the time for you, too busy, or over-worked). This is especially true if the accounting records are a mess or not currently maintained, because this condition is a cover-up by design. The operation is managed this way to discourage any review by managers and auditors. Press on.

After the fraud has been discovered and the perpetrator has been removed from the operation, revenue will quickly begin to increase or to appear from every imaginable source. Remember that management's first reaction to this condition is: "**Revenue is up**." A more accurate response is: "**Fraud is down**."

Every auditor must wear two hats in order to detect fraud.

(1) Cash Receipts. In cash receipting frauds, the transactions are not recorded. Therefore, the auditor must review for what is not there (experience). The attribute auditors must look for is that what you see is "too low".

(2) Cash Disbursements. In cash disbursing frauds, the transactions are recorded. Therefore, the auditor must review for what is too much. Fictitious transactions are concealed in large quantities, high volume, and big dollars. The attribute auditors must look for is that what you see is "too high".

FRAUD DETECTION METHODS - CASH DISBURSEMENTS

Perform a comparative analysis of expenditures from one period to another for each expenditure code or function. Analyze significant fluctuations (up and down), and select areas for further review accordingly.

Prove the mathematical accuracy of check registers. This step will detect plugged balances.

Compare the actual check register entry for critical data elements (i.e.; number date, payee, and amount) to the canceled check, voucher, and supporting documents for agreement. Review check endorsements carefully, especially dual endorsements on payroll or vendor checks.

Review check voiding procedures, and account for all copies of voided documents. Ensure that the signature block is excised (cut-off) for all signed, voided checks, and that all such checks are retained on file for reference and audit.

Review storage and issue procedures for blank (unnumbered) and prenumbered checks.

Review the authorization and approval process for check issuance. But, if this process exists, all fraud occurs after approval through falsification and alteration of documents.

Review the disinterested party bank account reconciliation carefully and for propriety.

Know the accounting entry for fraud in cash disbursement schemes, and look for it. What is it? The **accounting entry** for cash disbursements fraud follows:

Description	Debit	Credit
(Select one or more debits):		
Expense	XXXX	
Assets (inventory, or plant and equipment)	XXXX	
(Or):		
Revenue	XXXX	
Liabilities (accounts payable)	XXXX	
Fund Balance	XXXX	
(There is only one credit):		
Cash		XXXX

Expenses are commonly used because they disappear at year-end when the accounting records are closed and balanced. A comparative analysis of expenses must by used to identify what's too high or too much, because the fraud is often concealed in accounts with a high volume of activity or a high dollar amount.

COLLUSION

Collusion between entity employees presents a very unique situation. It doesn't happen very often, and is probably the last thing you'd think of during an audit.

- In a multi-person operation, the best opportunity to detect collusion is during a review of the entity's system of internal control. In addition to interviewing employees and documenting the system of internal control, auditors must perform substantive audit tests to evaluate reported controls to ensure that the system actually operates as intended and described. System variations may be honest misrepresentations of actual procedures (through oversight), or may be deliberate acts to conceal fraudulent activities. All deviations from prescribed policies and procedures should be investigated thoroughly.

- In a one person operation, there can be no true system of internal control, and collusion is not a factor. Auditors must rely on the results of substantive audit tests to detect irregularities or fraud.

When a perpetrator works alone to defraud an employer, this action is usually done in secret because the individual fears detection by others. By it's very nature, fraud is a covert activity. People just don't advertise their actions to other employees when they begin to manipulate entity records and documents for personal gain.

This is not the case when collusion is involved. Since perpetrators no longer have to fear detection by their fellow workers, they work openly to defraud their employer. When working in concert with another, perpetrators are able to carry out their plan of deception by willfully circumventing established internal control procedures. They do this to maintain illicit personal relationships and for personal financial gain.

While collusion doesn't begin overnight, it may happen quite naturally during a working relationship over a long period of time.

Each individual probably begins by taking something small from the organization. Money may not even be involved initially. But, as time passes, these two individuals notice each other doing whatever it is they're doing. They always share something in common. But, this common thread that binds these individuals together may never be detected by outsiders. Innocently they begin to rationalize by saying to themselves, and to each other: "It's all right to do what we're doing. After all, everybody does it." And, since neither one of these individuals can tell their employer about the other, they decide to go along their separate, but parallel paths.

Then one day something happens. These individuals somehow get together and really start doing things in a big way. This is where money usually enters the picture. If there is some type of personal relationship involved between these individuals, they probably say:

“Think what we could do with all the extra money. After all, we deserve it. The entity certainly doesn’t care what goes on here, because they never check anything we do. We certainly aren’t paid enough for what we do, and this affair is costly. If I’m not careful, my spouse is going to notice something is irregular in my financial situation.” All actions taken are fully justified, at least within the minds of the individuals involved. For them, it’s all right to do what they’re doing.

SEGREGATION OF DUTIES

Segregation of duties problems are the number one internal control weakness cited in fraud audit reports. No person should have control over a transaction from beginning to end. A simple sharing of duties between two individuals eliminates this weakness. In large organizations, this problem is usually dealt with on the basis of individual functions within the entity. However, in small organizations, this problem is dealt with on the basis of the entity as a whole.

- This sharing of duties is possible in large organizations. However, even large organizations have segregation of duties problems which are often overlooked by both managers and auditors. Prime examples of this include the accounts payable and payroll functions where one person is responsible for both preparing input (disbursement documents and vouchers), and receiving output (checks). This problem can be remedied by having the accounts payable and payroll employees switch some of their duties. For instance, the accounts payable employee inputs disbursement transactions into the system and receives the output from the payroll system, while the payroll employee inputs payroll transactions into the system and receives the output from the accounts payable system. This results in no increase in work or employee costs, but a significant increase in internal controls over entity disbursements.

- This sharing of duties is not possible in small organizations where there is only one person present in the entity. In many instances, only part-time employees work for the entity. This entity will never respond to a recommendation to hire additional people to accomplish this objective. Thus, the risk that fraud will occur and not be detected in a timely manner is extremely high under these circumstances.

When it's not possible or economical to have two people perform critical functions, a strong management review and oversight function accomplishes this same objective. Auditors often fail to recommend this solution to managers because they rationalize the problem away by saying that nothing can be done about the situation.

When frauds are analyzed, it's easy for managers and auditors to see how a lack of segregation of duties allowed it to be perpetrated. Many times the condition wasn't even noticed; but more often, no one ever attached any real importance to the condition. Internal controls are viewed with new meaning, and with a different level of significance when fraud occurs.

A lack of segregation of duties occurs when managers place too much trust in key employees. However, **BLIND TRUST** is usually the number one problem in fraud cases. These key employees are the same people auditors trust, and rely upon, during audits. When the trusted employee embezzles funds from the client, this is the person who provides the answers to internal control questionnaires, describes the work environment and other important aspects of the entity, and provides all the accounting explanations when account variances and deviations from standards are observed by auditors. To counter this threat, auditors must exercise due care and approach each engagement with a high degree of professional skepticism. Don't accept the first plausible explanation given by management for exceptions in audit tests. Follow-up to prove or disprove explanations given by the trusted employee.

THE TRUSTED EMPLOYEE

The trusted employee is indispensable to the entity. This is the person who: never goes on vacation; is never missing from the office except for very short periods of time (one day or less); always works early, late, or both; works weekends; reports to the office during those few times when a day off or vacation is taken, either by phone or in person; is the only person authorized to process transactions in excess of certain levels; or is the only person authorized to process transactions applicable to certain accounts. This climate gives the trusted employee the ability to manipulate the accounting records to keep any fraud from being detected.

The number one deterrent against the trusted employee who might commit fraud is a policy which requires all personnel to take vacations of a specified length of time each year. But, another employee must perform their job while they're gone, or the vacation requirement is of no value. Another way to accomplish this objective is to use cross-training which requires various individuals to exchange jobs for specified periods of time.

The most common attribute about frauds involving the trusted employee is that these key people were **ABSENT** from the work environment when the fraud was detected. Once removed, the relief employee who begins to perform this person's job quickly learns that the accounting records don't balance. They never have.

Removal of the trusted employee from the work environment can be either a voluntary or involuntary action. Normally, it's the latter. When the trusted employee is involuntarily removed, such as by some type of adverse personnel action or dismissal, the fraud is detected almost immediately because replacement personnel carefully analyze these functions. When the trusted employee voluntarily removes themselves from the function on a temporary or permanent basis, fraud is not always disclosed immediately, if at all, because newly hired employees rarely review work accomplished by their predecessors.

The trusted employee is usually the person who becomes involved in fraudulent activity. They didn't come to work planning to steal from their employer, and didn't even start embezzling soon after they were employed. But, they've been around long enough to see weaknesses in the system of internal control in their area of responsibility, and have been tempted beyond the level they can handle. As a result, they take advantage of the situation, and the entity, to profit personally.

BRIEF CHECKLIST TO IDENTIFY "AT RISK" EMPLOYEES

An employee with unusual work habits, such as an individual who:

- Comes to work early or leaves late.
- Works nights and weekends.
- Is seldom missing from the office, even to take leave or vacation.
- Reports to the office during brief absences (one day or less), by telephone or in person.
- Asks others to hold their work for them without processing it until they return.

Employees who are the only people who can authorize certain types of transactions, transactions in restricted accounts, or transactions in excess of certain levels. No one else performs these tasks if and when they're absent from the workplace.

An employee whose deferred compensation deductions are unreasonable given their living circumstances.

An employee whose spouse or significant other has recently lost a job.

Employees who are living beyond their means, such as those with lots of new "toys" (i.e.; cars, boats, travel trailers, motor homes, vacation property, home remodeling projects, etc.).

Employees who have high debt, such as those who are being "dunned" by creditors that frequently call them at the office in a collection campaign.

Employees who spend more money taking the staff to lunch than they make on the job.

Employees who brag about recent gambling winnings or family inheritances.

Employees who have a life style or pattern of gambling, and who frequently travel to gambling Meccas (they're probably losing).

Employees who "act out of character" by performing tasks which are not a part of their primary job duties.

Cashiers who always balance and are never over or short.

Cashiers who do not follow the organization's standard cash handling policies and procedures.

Employees who are always behind in their work and are content to exist in a "messy" work area. This is often by design and a mechanism used to conceal irregular or inappropriate activity.

Employees who are secretive on the job and are unwilling to let others review their work.

Customers frequently provide customer feedback about the employee’s errors and irregularities.

CASE EXAMPLES

Cash Receipts.

Collusion between the police chief and four successive municipal court clerks resulted in the loss of $45,300 in a small city. The police chief had an affair with each clerk, and finally married clerk number four. Clerk number three got upset over this change in loyalties and blew the whistle on the whole operation. What this clerk said was: "It's fine for us to cheat the city, but don't you ever cheat on me." These individuals embezzled cash receipts from various types of traffic citations. Using multiple cash receipt books, they stole seven out of every eight transactions in this scheme.

Collusion between two clerks resulted in the loss of $2,200 to a county senior center program. These individuals entered into a lesbian relationship, and embezzled cash receipts from client donations to the program to finance it. After leaving the employ of this entity, they continued to defraud subsequent employers in at least two other states.

Cash Disbursements.

Collusion between the supervisor of transportation and 13 bus monitors resulted in the loss of $114,400 in a school district. These bus monitors were legitimately hired by the supervisor through the district personnel system; but, they performed no work. Each person paid the supervisor a percentage split of their false wages. One of the bus monitors wound up in the hospital after the supervisor pistol-whipped him for not paying the required share of his fraudulent paycheck. This individual turned-in the supervisor from his hospital bed.

Collusion between a parts room employee, an assistant shop foreman, and the transportation supervisor resulted in the loss of $4,000 at a school district. These individuals circumvented the district's system of internal control over purchases by processing purchase orders and claims vouchers for personal items through the district's disbursement system. They used their public office to obtain small buildings, tools, clothing, equipment, and landscaping materials for personal gain. A complete inventory of all parts, supplies, materials, and equipment was not maintained in the transportation department, and there was a complete lack of accountability and responsibility over the department purchasing function. An anonymous transportation department employee got fed up with the abuse of the system and reported these fraudulent activities to the district. What this employee really said was: "I'll tolerate a little bit of theft, but not a whole lot of theft."

Collusion between a counselor, a quality control clerk, and two private citizens resulted in the loss of $3,000 in a county assistance program. These individuals set up an office assembly line to falsify applications for energy assistance. Payment checks issued for these bogus benefit authorizations were subsequently cashed. The proceeds were split between the participants in this scheme.

FRAUD/HIGH RISK DECISION PROCESS (AUDITOR MIND SET)

(1) WHAT IS THE SCHEME?

Review the internal control structure
Identify audit risk(s)
Determine what could go wrong for each identified audit risk
Identify potential fraud scheme(s)

(2) WHAT DOES IT LOOK LIKE?

Analyze audit risk(s) and describe the potential fraud scheme(s)
Determine the key attributes of the fraud scheme(s)

(3) DOES IT EXIST?

Determine what audit test addresses each identified attribute of the fraud scheme(s)
Perform the audit test(s)
Reach a conclusion about the existence of the fraud scheme(s):

(a) Fraud exists (an effect of poor internal controls)

(b) Internal control weakness exists only (no fraud effect)

A SUGGESTED INTERNAL CONTROL GUIDE FOR MANAGEMENT OFFICIALS

(1) Reporting Fraud.

State agencies and local governments in the state of Washington are required to notify the State Auditor's Office when losses are suspected or detected (RCW 43.09.185). The statute includes losses of money and other assets, as well as illegal acts.

General Requirements:

(1) Notify the State Auditor's Office if you suspect or detect fraud or other irregularities. Ensure your entity has a policy to implement the reporting requirements of the statute.

(2) Protect the accounting records from destruction.

(3) Don't enter into a restitution agreement with an employee prior to an audit to establish the amount of loss in the case.

(4) Ensure that any personnel action is taken based on the employee not following your policies and procedures, rather than for misappropriating public funds (civil versus criminal).

(5) File a police report with the appropriate law enforcement agency when advised to do so by the State Auditor's Office.

(2) Segregation of Duties.

No employee should control any transaction from beginning to end. When it's not possible to segregate duties between two or more employees, establish a periodic monitoring program for this key employee that effectively accomplishes a segregation of duties without hiring another individual to perform the task.

The internal control structure self-destructs when primary personnel leave their workstation during breaks and lunch. During this time period, relief personnel perform too many functions.

No one reviews the work of supervisors, and the risk of loss increases when these individuals have the ability to perform (or actually perform) sensitive tasks in the cash receipting and cash disbursing functions. Supervisors ("reviewers") perpetrate just as many frauds as the first line employees performing critical functions ("doers"), and they usually responsible for cases that occurred over a long period of time and involved the largest dollar losses. Someone must take a "last look" at this key employee and review their work in the same manner the supervisor monitors the work of others.

Don’t tempt employees, and don’t put them at risk in a poor internal control environment or an internal control environment that is not properly monitored.

Everyone has the ability to do something, usually what they have access to and can control. The root cause of fraud is a financial need at home (MOTIVATION). The root cause of fraud in the entity is a lack of segregation of duties and lack of monitoring of employee activities by management officials that gives the employee the opportunity to perform an irregular act and conceal it for long period of time without detection (OPPORTUNITY). Opportunity plus motivation (and sometimes greed and poor internal controls) equals FRAUD. Employees justify their irregular activity in their own mind.

(3) Cash Receipting - All Locations.

Make bank deposits daily (every 24 hours) and intact (in the form you received the funds). This eliminates the opportunity for employees to delay deposits and play the “mix and match game” with the contents of multiple deposits and unrecorded funds from various miscellaneous revenue streams.

Make sure you can fix responsibility for funds to a particular employee, at a particular point in time, all the time. Major problems include: (a) operating with multiple cashiers on a cash drawer and commingling funds; (b) having unrestricted access to funds in safes and vaults; and, (c) using poor cash transmittal systems from one level of the entity to another.

Properly protect safe and vault combinations, as well as computer passwords where the controls are the same. Limit access to the combinations and restrict password access to certain programs as necessary, change them periodically and when employee terminate employment, and don’t write them down anywhere in the office.

Perform unannounced cash counts of all change funds and imprest fund accounts on a periodic basis. Ensure overages and shortages are reported in the accounting system as miscellaneous income and expense. Monitor activity by cashier for unusual trends. If you hold employees accountable for overages and shortages, you’ll cause them to take irregular actions to make sure everything balances. Review all checks to ensure that personal checks from employees are not present (“borrowing’, or using the fund as a check cashing facility) and that unrecorded revenue checks are not present.

Perform an analytical review of all revenue (the same is true of payroll and general disbursements as well), and the lower the level of analysis with the entity, the better. Fraud perpetrators routinely take all (or practically all) revenue from specific revenue streams. Ensure all revenue streams are properly included in the entity budget and that someone monitors actual revenue versus expectations.

Use official prenumbered cash receipt forms with the government name printed on them rather than generic receipt forms (i.e.; Rediform, etc.) that can be obtained from any office supply store.

Perform a review of the sequential issue and use of official prenumbered cash receipt forms and cash register "Z" tapes (total accountability).

Record mode of payment (i.e.; check, cash, or money order) in the cash receipting system. Agree total cash receipts by mode of payment from the accounting records to a **bank-validated** deposit slip that lists the check and cash composition of the actual deposit.

All checks should be restrictively endorsed "For Deposit Only" immediately upon receipt by cashiers, and all revenue transactions should be recorded at the initial point of entry into the entity. Funds received at one location should not be transmitted to another location where another person subsequently receipts them. A person who does not receive the money first is most often involved in misappropriating incoming revenues. Create an appropriate audit trail.

Ensure void, refund, and paid-out transactions are authorized and approved by a supervisor and supported. Ensure that exception reports are prepared for all non-cash credit transactions, approved by a supervisor, and appropriately supported.

As with any computer cash register system, manual cash receipt forms are required for power outages and system maintenance (scheduled and unscheduled). Verify that manual cash receipt forms are cross-referenced and all transactions are subsequently entered into the computer accounting system for accountability purposes.

Two individuals should open the mail, make a log or record of the transactions, turn these checks over to the cashier function, and then reconcile the log to daily cash receipts and the bank deposit to ensure that all transactions have been properly accounted for and controlled. An alternative solution is to use a bank lock box for large revenue streams.

(4) Decentralized Location Cash Receipting.

Direct deposits to the bank are preferable.

If funds are transmitted to the central treasurer function, review sequence and continuity of turn-ins and determine how the universe of all transactions is monitored. Determine whether the amount of cash receipts recorded at the central treasurer function agrees with the amount of funds collected at decentralized cash receipt locations. Review decentralized location reconciliations of revenue collected versus revenue recorded. Employees first perform this task by reviewing the "come-back" copy of any transmittal form and/or a receipt from the central treasurer. But, they must also review the accounting reports to ensure that the correct amount of revenue was recorded for the function. This reconciliation is critical and monitors the completeness and accuracy of transaction processing at the central treasurer function.

Have two people present to count turn-ins when funds are transmitted from decentralized locations to the central treasurer function.

Immediately count and receipt turn-ins when funds are hand-carried to the central treasurer function. Obtain a receipt for all fund transfers.

Verify mode of payment for all transactions included in bank deposits.

Use locking or tamper proof deposit bags for transmittals and deposits.

Maintain a courier signature log for deposit bags hand-carried to the central treasurer function and to the bank. Fix responsibility for funds to a specific individual at all times.

Prepare a Daily Activity Report that captures accountability information from all funds and documents for monitoring and tracking purposes. This includes: cash receipts (the actual money), "Z" tape numbers from cash registers, prenumbered cash receipt forms issued, inventory, etc.

(5) Accounts Receivable.

Agree control and subsidiary accounts. The control account is written down to agree with the total of all subsidiary accounts to conceal fraud.

Agree total subsidiary account credits from cash collections to bank deposits (revenue).

Agree total customers per meter books to total active customers on the system. The use of hand-held computers by meter readers eliminates input manipulations.

Ensure cancellations, adjustments, and other write-off transactions are authorized and approved by a supervisor and properly supported. Remember that the employee who has the access and capability can perform this task 24 hours a day, 7 days a week, 365 days a year whether the actions are authorized or not. Prepare and monitor system generated exception reports listing these high-risk transaction types.

Fraud may be concealed in delinquent (no pay) accounts. Confirm large receivable amounts and delinquent accounts with customers. Confirming the date and amount of the last payment or payments over a period of time may be more beneficial than confirming the amount of the delinquent account balance because the amount of the delinquency is not always known by the customer. Employees conceal delinquent balances from customers by stealing the statements (i.e.; obtaining the system generated statement either inside or outside the organization, preparing a manual statement showing current charges only, and then mailing the statement to the customer).

Fraud may be concealed in slow pay accounts. Confirm late cycle payments with customers. There is no other way to determine the existence of a lapping scheme when cashiers do not make mistakes.

Review rates for those other than authorized (i.e.; flat rates versus computations based upon meter readings).

Determine if the entity knows the percentage of customer payments made in cash, and whether this expectation is being met. Determine if there is any (or a sufficient amount of) cash in bank deposits.

(6) Payroll.

Payroll expenses represent 50-75% of all disbursements in government.

Perform a ghost employee test using a payroll list versus making a payroll payout. Confirm that employees exist with department employees not performing payroll or leave functions. High-risk areas are part-time employees and those who have terminated employment but are still getting paid.

Determine if employees are paid more than authorized. Compare W-2 amount to the employee's actual salary. Review the payroll clerk's records for all types of payroll transactions, particularly in small entities, because this is the highest risk area.

Ensure mid-month payroll draws are authorized and deducted from end-of-month pay. Review the payroll clerk's records, particularly in small entities.

Ensure overtime and stand-by time are authorized and supported. Stratify the population to identify heavy users for subsequent analysis and testing. Departmental timekeepers and any supervisor who approves his/her own time sheet are high risk employees.

Ensure sick and annual leave accruals and compensatory time uses are in accordance with entity policy and properly input/recorded in system after approval. Determine whether balances are retained in excess of that authorized. Departmental timekeepers are high risk.

Compare the amount, payee, and endorsement on redeemed warrants to the actual warrant register for a specified period of time (block sample). Multiple endorsements are high-risk documents.

Look for straight line from source (employee) to approval (supervisor) to payroll (payment) for all time cards/sheets. All fraud is after supervisor approval when time cards/sheets are returned to the employee. (The same is true of travel vouchers and petty cash vouchers.) The highest risk employees are departmental timekeepers (who alter their time sheets after approval by managers), managers (whose time sheets may not be approved by anyone), and employees who work in the payroll function (who manipulate their own payroll records).

(7) General Disbursements.

Evaluate the auditing officer and governing body approval process for propriety.

> The auditing officer function serves as an outstanding review mechanism for entity disbursements, as long as the auditing officer is at the proper level within the organization and the review is performed with interest.
>
> The approval function by the governing body can be perfunctory because members are not necessarily trained regarding what they should be looking for or the purpose of their actions. Approval of general disbursements by the governing body is not a guarantee of transaction validity.

Employees with input and output responsibilities are the "kiss of death" in disbursements systems (accounts payable and payroll functions). Switch duties of each person in these functions to eliminate this conflict.

The accounting entry for disbursement fraud is debit expense, assets (inventory or fixed assets), revenue, liability (accounts payable), or fund balance and credit cash. Identify what's too high or too much (comparative analysis of expenditures). Fraud is concealed in accounts with a high volume of activity or high dollar amounts.

Eliminate the use of blank lines on time cards, petty cash documents, and travel vouchers (i.e.; crossed out) after approval. Otherwise, these types of documents serve the same purpose as blank checks. All fraud is after approval through alteration when the documents are returned to the employee preparing them.

A missing or fraudulent (altered) document is at the heart of every fraud. Don't use the FIDO concept, "forget it, drive on" when missing documents are encountered. Find the real reason.

The greatest disbursement risk is represented by manual transactions that occur between periods represented by computer generated warrant registers. These manual transactions may be shown as pen and ink changes to computer generated warrant registers, may be omitted entirely, or may represent duplicate warrants previously processed through the system. The governing body may not have even approved these transactions.

In state agencies, most disbursement fraud cases have been detected in the smaller disbursement systems rather than in the larger systems. In smaller entities, this would equate to a risk in a purchasing imprest fund.

Review a sample of entity disbursements for propriety. Scan the warrant register for any unusual items. Since normal expenditures are repetitive in nature, concentrate on variances from the norm.

Review disbursements for fictitious vendors, duplicate payments, overpaid employees, and payments to "cash" or financial institutions. For false vendors, compare like data elements from the personnel/payroll system to vendor files. Review invoices for

Rediform documents, prenumbering (make sure you don't get all the numbers, as in the only customer), post office box addresses only, lack of telephone numbers, etc.

Compare the amount, payee, and endorsement on redeemed warrants to the actual warrant register for a specified period of time (block sample). Multiple endorsements are high risk documents.

Look for straight line from the initiator of the transaction to the accounts payable function to check/warrant distribution. All fraud is after processing when checks/warrants have been returned to the initiator, a compromise of the internal control system. Reasons given are emergencies and meetings with the vendor, and employees use "post-it notes" or other verbal/written messages to accomplish this, indicating that emergencies and meetings with the vendor are the reasons for this action. Prepare a manual exception report for all "U-Turns" either at the accounts payable function or the check/warrant distribution function to identify the universe of all transactions processed outside normal parameters. Periodically review the supporting documents for these transactions for trends, and examine the bank endorsements on the checks/warrants for validity.

Review access controls to ensure that no employee can initiate disbursement transactions, release the batch of transactions to request production of checks, and then pick-up or obtain the checks/warrants.

Use of "pseudo vendor codes" (i.e.; one-time payments in lieu of establishing valid vendor codes) should be documented on an exception report. Periodically review the supporting documents for these transactions for trends, including any abuse of the system such as multiple payments to the same vendor.

Prohibit either accounting functions from being performed in the data processing function, or vice versa. Accounting department personnel should not have the authority to make computer software changes to any program, such as the check redemption software program. In addition, accounts payable duties should not be performed by anyone outside the accounts payable function.

Ensure managers close monitor all disbursement transactions initiated by anyone working in the accounts payable function or by an individual totally in control of the disbursement function in a small organization, such as an executive director or financial officer.

Ensure managers close monitor all refund transactions disbursed by check/warrant. These transactions represent "negative cash" and are inherently high risk for fraud.

Examine vendor contracts in cases where the transaction analyses or analytical review procedures suggest high, increasing, or unusual volumes with specific vendors. For example, sort all expenditures by vendor by accounting year and list them from highest to lowest dollar amount and review for unexpected variances. If vendors are selected by competitive bidding, review underlying contract selection files to determine if there are valid documents on file.

For purchasing transactions, determine if assets are signed-for as received and signed-for as authorized for payment by two different employees. Identify the name and position of the individuals involved. Employees act out of character by doing something that is not a part of their normal job description when fraud is involved.

(a) Imprest Funds.

The next greatest risk for expenditure frauds comes from transactions that have been processed through imprest funds (i.e.; petty cash, purchasing, etc.) before being reimbursed by check/warrant. Review a sample of imprest fund reimbursement transactions for propriety. (Note: These same concepts also apply to all types of expenditure documents.)

Review for use of original source documents only.

Review for falsified (i.e.; "cut and paste") documents in the file.

Review for validity of supporting documents.

Review for appropriateness of supporting documents for entertainment and meals. Budgeting, Accounting and Reporting System (BARS) Manual requirements include a list of those present and the official public purpose of the meeting.

Review for continuity of reimbursements (dates and/or numerical sequencing of checks issued).

Determine whether all reimbursed documents are marked "Paid" to preclude their reuse.

Determine whether any disbursement transactions are stale dated.

Determine whether the fund is reimbursed timely (i.e.; monthly) and at year-end.

Determine whether the authorized fund level is appropriate (i.e.; 2.5 times the monthly expenditure level).

Scan the deposit and disbursement activity of imprest fund accounts for money laundering activities, such as:

Depositing unrecorded revenue checks into checking accounts.

Writing checks to "cash", "blank", self, a financial institution (for a money order or cashiers check), or a fictitious vendor (paying personal bills).

Making "cash back" withdrawals from bank deposits.

(b) Travel.

Travel fraud occurs when one employee violates entity policies and procedures. It is not a systemic issue within the organization. Key managers, department heads, elected public officials, and employees in the accounts payable function are the highest risk employees. Travel irregularities have occurred by:

The entity uses the actual expense system rather than the standard state per diem system. Use of the actual expense system is costly for management to review and for auditors to evaluate, with no significant improvement in the quality of supporting documentation. In addition, employees are encouraged to falsify receipts for expenses to obtain reimbursement for items that are not otherwise authorized when actual expense systems are used. Sequential receipts are submitted for expenses at various establishments in multiple cities.

Employees file personal travel vouchers with more than one organization for the same expenses. Original documents are filed with one organization, while copies are filed with the other organization. One entity should serve as the source of all original documents and then bill the other entity for its share of authorized expenses.

The government allows hotels to direct bill them for room charges of employees, but does not compare hotel billings with employee travel vouchers for duplicate payments.

Employees incur unauthorized expenses or purchase gifts and alcoholic beverages in violation of entity policies.

Employee vicinity travel vouchers are not compared to travel vouchers filed for other specific events, or to the employee's time sheet and telephone records due to the timing differences in receipt of these documents by managers and supervisors. Periodically review all documents together for specific high risk employees. Duplications or other irregularities occur, such as vicinity travel while out of town on other official business, vicinity travel while not on duty, and vicinity travel when the employee's telephone records indicate a presence in the individual's primary office (i.e.; travel not likely or probable). Determining the individual's physical "imprint" at the office is critical to understanding what really occurred.

Travel vouchers for specific events include payment for meals that were provided by the sponsoring organization. Ensure procedures include the requirement for conference agendas to be filed with travel vouchers.

Inappropriate supporting documents were filed with the travel voucher. These include copies of documents rather than originals, charge slips rather than actual receipts, etc.

(c) Purchasing/Credit Cards.

Purchasing/Credit card fraud occurs when one employee makes personal purchases in violation of entity policies and procedures. It is not a systemic issue within the organization. Specifics follow:

There were no policies and procedures for the control, issuance, and use of credit cards. Employees did not sign an agreement indicating an understanding of the entity's policies and procedures regarding allowable uses for credit cards. Entity training is critical to success.

The entity did not maintain a log of all credit cards issued, including the signature of each custodian.

The entity paid its bills using only the credit card statement.

Original customer sales receipt documents were not obtained or retained to indicate what was purchased, who purchased it, and the official business purpose. Receipts included only the total amount of the charge without any detail provided on what was purchased. No determination could be made as to whether or not purchases were legal or allowable. An itemized expense voucher was not used for purchases. Xerox copies of credit card charge slips were turned-in as support for expenditures. Use original source documents only.

For gasoline credit cards, a log sheet was not used for each vehicle to record the date of the transaction, amount of fuel purchases, mileage of the vehicle, and the name of the purchaser. No one monitored vehicle usage (i.e.; such as comparing gallons of gasoline purchased versus mileage driven over a period of time).

(d) Telephone.

All telephone [i.e.; State Controlled Area Network (SCAN), Sprint-Plus, etc.] fraud occurs when one employee makes personal calls in violation of entity policies and procedures. Specifics follow:

There are no records maintained on personal local calls in these systems. Some use is normal and to be expected; but, the use must be reasonable as determined by entity policy. Monitoring is the important issue.

Block access for international calls from all employees except where such use would be normal or expected (i.e.; key executive levels only).

Monitor monthly long-distance telephone bills for employees promptly. Scan statements for unusual activity such as calls before or after normal duty hours and out-of state calls.

Personal long-distance telephone use and cellular telephone use must be monitored. Ensure all employees certify monthly statements that all telephone calls are for official business purposes. Identify abuses promptly, seek reimbursement of all personal expenses, and take appropriate personnel actions as deemed necessary when abuses occur. Entity training classes for employees is critical to success.

Monitor monthly cellular telephone use to ensure that employees are enrolled in the appropriate plan for the amount of time actually being used. Reduce plan minutes purchased if actual employee use does not justify continuing with the original plan selected. Increase plan minutes purchased if actual employee use consistently exceeds the original plan selected. The objective is to obtain telephone services at the least cost.

(8) Bank Accounts.

Confirm cash and investments with financial institutions. Inquire of banks in the area for any unauthorized or "off book" savings or checking accounts in the name of the entity (i.e.; look like or sound like the entity name).

Ensure that an independent party performs (preferably) or reviews the monthly bank reconciliation in a timely manner and receives the bank statement unopened and directly from the bank. Review all canceled/redeemed checks for any bogus checks that were never issued, and any other irregularity. Fraudulent transactions noted within 30 days after the statement date are the bank's liability; however, if not detected promptly, these transactions become the entity's liability. Use positive pay or reverse positive pay systems to promptly reconcile checks/warrants issued versus checks/warrants being cleared at the bank. Block electronic or debit transactions, either completely or selectively, as appropriate. Ensure entity check/warrant stock meets industry standards.

See paragraph 7(a) above on imprest funds. Review all accounts for money laundering activities.

(9) Trust and Suspense Funds.

These funds are present in courts (bail), sheriff's office (inmate trust and confidential fund), county prosecuting attorney's office (racketeering fund), treasurer's office (treasurer's trust, advance taxes, and current taxes), coroner's office (deceased person trust), hospitals (trust), etc.

Verify that accountability equals the amount of funds on-hand or in the bank.

Review transaction additions and deletions to the account to supporting documents.

Compare canceled warrants/checks to the warrant/check register for agreement of payee, date, and amount. Review warrant/check endorsements for dual party signatures and other irregularities.

See paragraphs 7(a) and 8 above on imprest funds and checking accounts. Review all accounts for money laundering activities. Ensure all activity is authorized.

(10) Retail Sales Activities.

Plan for success, not failure. Establish policies and train staff. Ensure that all fund-raising activities are authorized. Establish internal control procedures to be used for each activity in advance. Determine what types of forms or other mechanisms will be used for control and accountability purposes. Hold employees accountable for following entity procedures and for all funds. Fix responsibility for funds to a specific employee at all times. Ensure that daily activity report forms are prepared.

Ensure that gross profit testing is performed and documented for all fund-raising and retail sales activities, and monitored by entity officials to ensure revenue expectations were met. These include soft drink machines, candy sales, school stores, other retail sales activities, and other items.

Always have two people empty funds from vending machines of all types. These funds should be counted immediately and receipted by the treasury function.

Use prenumbered theater tickets for attendance activities.

Use prenumbered customer signature sheets for other miscellaneous revenue streams and make the customer a part of the internal control system.

These same concepts also apply to all types of locally generated revenue

(11) Inventory and Fixed Assets.

Secure storage facilities and limit access. Maintain a record of all responsible individuals and keys.

Maintain a perpetual inventory record showing all purchases and issues. Take and document a periodic inventory (fixed assets, controlled substances, resale merchandise).

Verify usage to other entity accountability records (repair orders, vehicle records, patient records, etc.).

Tag all fixed asset acquisitions (identify through disbursement system).

Account for surplus property from time of declaration, through approval, to actual disposal and receipt of revenue, if any.

Control all recycle materials to ensure receipt of funds after disposal.

(12) Use of Entity Resources for Private Gain.

Establish and enforce entity policies stating that resources (i.e.; facilities, telephones, electronic mail, computers, equipment, supplies, vehicles, etc.) may not be used for private gain. Periodically monitor these areas for compliance.

(13) Entity Communication Program.

Since off-book purchasing frauds are found as a result of tips and complaints, the entity must have an internal and external communication process.

Restrict access to buyers by using a central vendor reception area.

Inform vendors of entity policies regarding gifts to employees and conflicts of interest. Send an annual "holiday" letter to vendors to remind them of this.

Hire competent and honest employees. Conduct background investigations and verify employment application information (i.e.; educational degrees, certifications, and references). The entity should research the public records for prospective employees to determine if they have a prior criminal history.

Clearly define permissible and prohibited employee conduct.

Establish a good system of internal control.

Notify employees of entity policies and procedures. Advise employees they cannot use company property for personal gain, participate in certain types of outside employment, or accept gifts, favors, travel, or entertainment from vendors.

Require signed annual employee conflict of interest statements.

Establish employee early-warning mechanisms, such as complaint systems and a whistleblower program (Chapter 42.40 RCW, state agencies; and Chapter 42.41 RCW, local governments).

Other items might include an employee suggestion and incentive programs, a hotline, employee exit interviews, and periodic questionnaires/surveys for employees and vendors.

Use the internal and external audit function when irregularities are detected.

Advertise successful prosecutions to employees and vendors as a deterrent measure.

(14) There's More.

You are limited only by your imagination and interest in a specific area of entity operations.

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

Cash Receipt Fraud Schemes

- Check for Cash Substitution Scheme
  - Case Study: Affiliated Health Services (Hospital)
- Lapping Scheme
- Accounts Receivable Schemes
  - Method of Documenting Accounts Receivable Losses
  - Summary of Major Areas of Concern in Accounts Receivable Systems
  - Accounts Receivable – Internal Control Structure – Duties of Personnel
  - Accounts Receivable Fraud Cases
  - Typical Accounts Receivable Fraud Scenario
  - Case Study: Highline Water District
  - Case Study: City of Battle Ground
  - Case Study: City of Poulsbo Municipal Court
  - Case Study: Edmonds School District Business Office
- Cash Register Schemes
- Computer Cash Receipt Schemes
- Cashiers Who Place Personal Checks in the Till Drawer
- Cashiers Who Collect the Money and Steal It
- Cashiers Who Establish Their Own Accountability
  - Case Study: WSU Animal Sciences Department
- Cashiers Who Alter Cash Receipts After Issue
- Cashiers Who Use Multiple Receipt Books
- Cashiers Who Make Short Deposits
- "Free" Access to Safes and Vaults and No Fixed Responsibility
- No Decentralized Direct Deposits
- Retail Sales Activity Schemes
  - Critical Path for Success in Any Associated Student Body Fund
  - ASB Fund Common List of Concerns
  - ASB Funds – What is Public Versus Private Money
  - Internal Controls Over Retail Sales Activity
  - Training Example
  - Retail Sales Activity Loss of Funds Case - Associated Student Body Fund
- Checking Account Schemes
- Establishing Bogus Entity Checking Accounts

CASH RECEIPT FRAUD SCHEMES

CHECK FOR CASH SUBSTITUTION SCHEME

A check for cash substitution scheme is the number one way funds are stolen in any cash receipting activity. This scheme is perpetrated by a cashier or accounting clerk who substitutes checks from unrecorded payments for cash from payments which have been receipted and recorded in the accounting records. When the cashier places the checks from these unrecorded transactions in the cash drawer, there is an immediate overage in the account. To remedy this situation, the cashier merely removes the displaced cash from the cash drawer. These funds are simply stolen.

Substituting checks for cash, dollar for dollar, is the most common method used by cashiers to misappropriate funds. Substituting checks for cash on less than a dollar for dollar basis is not quite as simple, and isn't done as often. In these cases, the full amount of the check is deposited in the bank, while a receipt is issued for any amount less than the amount the customer actually paid.

The checks used in this scheme are almost always received through the mail. These are high risk transactions because these customers do not ever expect to receive a receipt. Their canceled check is their receipt. The customer's account for each unrecorded transaction is always marked "paid".

Red Flags:

- Employee duties are inappropriately segregated.
- Deposits are not made daily or intact (i.e.; in the same form received).
- The check and cash composition of the daily bank deposit doesn't agree with the mode of payment indicated on the issued cash receipts (i.e.; less cash and more checks).
- Managers do not conduct periodic unannounced cash counts at all cash receipting locations.
- The entity uses commercially purchased or variety store cash receipt forms (i.e.; rediform, generic, etc.) rather than official prenumbered cash receipt forms (i.e.; entity name printed on the form) in the cash receipts function. These forms are obtained from office supply stores and provide no control over cash receipts.
- Managers don't account periodically for and control the official pre-numbered cash receipt forms issued to each receipting function or verify that these forms are actually being used sequentially. This review should also account for all copies of voided forms, as well as monitor the sequential use of "Z" (total accountability) tapes produced by manual or computer cash registers.
- The entity uses cash receipt forms which do not indicate mode of payment data (i.e.; payment by check or cash).

- The organization doesn't verify daily cash receipt accountability to a bank-validated deposit slip showing check and cash composition.

- The organization doesn't control revenue checks which are received through the mail by having two employees open the mail, make a log of the transactions, and then reconcile this information to daily cash receipt transactions to ensure that all payments were recorded properly and deposited in the bank.

Fraud Detection:

- Review the segregation of duties of key personnel.

- Review the check and cash composition of the daily bank deposit during unannounced cash counts and during substantive audit tests of cash receipts. (This review should also be performed periodically by management.)

- Review the entity's records of the numerical series of official prenumbered receipts issued to each function, and verify that these receipts are used sequentially (including properly accounting for all copies of voided documents).

CASE EXAMPLES

Municipal court cashiers stole $1,000 and $5,200, respectively, from customer traffic citation payments. Both frauds were detected by auditors. While checks from transactions received through the mail were included in bank deposits, no cash receipt forms were issued to these customers. The court did not periodically review the check and cash composition of deposits, and did not reconcile total tickets issued by the police department with total tickets processed by the court. A 19 year old teenager began stealing money on day 8 of employment at one of these entities.

A sanitary landfill cashier stole at least $200 from user fees collected for garbage disposal. Auditors performed an analytical review or revenues and detected an unexplained $12,000 revenue decline from the prior year (i.e.; no change in number of customers or rates). Checks were included in the landfill bank deposits from people and in amounts which did not correspond to cash receipt forms issued (i.e.; no cash receipt was written to Jones for a $100 payment, but the $100 check from Jones was included in the bank deposit).

A city clerk and a school district secretary stole $400 and $3,600, respectively, from miscellaneous revenue transactions. Both frauds were detected by auditors. Checks were included in the district's bank deposits from people and in amounts which did not correspond to cash receipt forms issued.

A sheriff's department cashier stole $7,000 from user fees collected from the sale of accident reports to the public. Entity managers detected this fraud after another cashier became suspicious of unusual transactions. Checks received through the mail from insurance companies

and attorneys to obtain copies of accident reports on their client's behalf were not receipted, but were included in the department's deposit with the central treasurer.

Affiliated Health Services (Hospital) - $213,668 – 3Years

Scheme. A general ledger technician committed a check for cash substitution scheme to manipulate the hospital's daily bank deposit. Decentralized locations at two hospital district recorded mode of payment on cash receipts issued and summarized this information on daily accountability reports for cash collections. Some of these locations did not issue cash receipts for certain types of collections. But, all funds were transmitted to the central administrative office where the bank deposit was prepared. The employee kept unrecorded revenue checks from these areas in her desk ($48,000 at the time of our audit). These checks were then substituted for currency received from the cafeteria, the primary location receiving currency each day. No one verified the check and cash composition of the daily bank deposits or otherwise monitored the work of this technician.

Detection. Routine SAO audit in cash receipts testing and review of the hospital's internal controls over cash receipts. The check and cash composition of the daily bank deposits did not agree with the mode of payment on the cash receipts issued by the decentralized hospital locations. There were more checks and less currency in the bank deposits, the primary attribute of a check for cash substitution scheme.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Segregation of duties problem. The general ledger technician gained access to the hospital's mail and computer records over time (job creep). In addition to her duties in preparing the bank deposit where she had access to all hospital revenue, she also had access to patient and other hospital billing records where she had authority to process account adjustments. Her work was not properly supervised by managers.

(2) The district did not properly control checks which arrived through the mail, and internal controls over cash receipts were inadequate. No one compared the mode of payment from the cash receipts issued and daily accountability reports to the check and cash composition of the daily bank deposit for agreement.

(3) There was very little cash in bank deposits; but, large amounts of currency were routinely received from the hospital cafeteria.

(4) Checks were not always receipted at the point of entry at all of the hospital's decentralized operating locations.

(5) Miscellaneous commercial account adjustments were not promptly review by managers.

Detection Steps.

(1) Review employee duties to determine if one individual is able to control transactions from beginning to end, particularly in the cash receipting function. Determine whether managers review the work of the person preparing the bank deposit in the same way the employee reviews the work of others.

(2) In cash counts and cash receipts testing, compare mode of payment information from daily accountability documents to the check and cash composition of the daily bank deposit.

(3) Review accounts receivable adjustments to determine if they are authorized, approved, and properly supported. Determine if an exception report is prepared for all account adjustments for management oversight purposes.

(4) Review procedures for processing mail. Determine if two people open the mail, make list/log of all checks received, and then compare revenue received to subsequently prepared cash receipt and bank deposit records.

(5) Perform analytical reviews of revenue streams and miscellaneous revenue for reasonableness and agreement with expectations.

Sentencing. The general ledger technician pleaded guilty to first degree theft and was sentenced to one year in jail at the Washington State Department of Corrections at Purdy. Exceptional sentencing guidelines were used.

TRAINING EXAMPLE

The attached case example clearly demonstrates how a review of the composition of a daily deposit will detect a check for cash substitution scheme. While this is not an actual fraud case, all frauds look exactly like this.

There were 3 receipts issued on the date in question, January 15, 1988. The receipts used are official prenumbered receipts which indicate mode of payment information, and were issued in numerical sequence. These represent 100% of the transactions for this date. Each transaction represents $1,000 in cash receipts. Two of these transactions were paid by cash (Jones and Adams), and one transaction was paid by check (Smith). Take the following steps:

- Add up the total amount of cash receipts for this date ($3,000) and agree this to the deposit total ($3,000). Since these amounts agree, this entity deposits cash receipts intact daily. If this is where your cash receipts testing normally ends, you're making a serious mistake. If you stop here, you've missed the fraud! The cashier you're auditing will now be able to continue perpetrating this scheme in this entity. So, don't let this happen to you. Keep going!

- Add up the amount of cash (i.e.; currency) received for the day ($2,000). Compare this amount to the actual cash deposited for this date ($1,000). If these amounts agree, your

composition review is finished. If not, you have additional audit work to perform. In this case, the amount of cash deposited ($1,000) was less than the amount of cash received from the recorded cash receipts ($2,000). Thus, on this date, there is an unreconciled difference of $1,000 (more cash was received than was deposited). When these variances occur, you must analyze the actual checks recorded on the deposit slip to determine which checks do not belong there. In a fraud case, this will identify the universe of unrecorded cash receipt transactions which have been included in the deposit on this date. In this case, the check for Smith is properly shown on the deposit slip. But, the check for James does not belong in this deposit. There was no cash receipt written for James on this date.

- Contact the entity's bank. Request a copy of the check for James from the bank's microfilm record of deposits so that additional audit work can be performed. It is not necessary to order copies of all checks shown on the deposit slip for days with variances. Once the check for James is obtained from the bank, you need to determine why it was included in the subject deposit. The fact that the check is located in the deposit does not necessarily mean that fraud exists. There could be a valid reason for this condition.

    - If a fraud is not involved, the check may be from one of the following sources: (a) a personal check cashed by an employee or other individual; (b) a check from another source of revenue commingled with this deposit (the fraud may be in another function); (c) a check for an amount greater than a legitimate customer payment (i.e.; less than $10 over the amount due on the account); or (d) some other miscellaneous valid and explainable reason, such as an error made in recording the mode of payment on the cash receipt form. Items (a) and (c) above must have an entity policy covering the conditions under which these situations will be permitted.

    - If a fraud is involved, the check represents an unrecorded payment made by a customer (check for cash substitution scheme). In an accounts receivable operation, your additional research will indicate that the customer's account (individual subsidiary ledger card) has been marked "paid" for the transactions in question. In a municipal or district court, the customer's traffic citation for this transaction will be marked "paid" (perhaps by canceling, voiding, dismissal, etc.) and filed in the completed file. In this example, the extra check for James does, in fact, represent an unrecorded transaction. Thus, the cashier in this entity is operating a check for cash substitution scheme.

- Compute the amount of the loss as follows: First, determine the correct amount of total accountability for this date. In this example, you must add the unrecorded transaction for James ($1,000) to the total of the recorded transactions for Jones, Adams, and Smith ($3,000) to determine total accountability ($4,000). Next, subtract the amount of the daily deposit ($3,000) from the correct total accountability ($4,000). Finally, this calculation gives you a difference of $1,000 which represents the cash shortage in this account. Therefore, this example involves a fraud where $1,000 in public funds was stolen by a cashier on this date.

ATTACHMENT: CHECK FOR CASH SUBSTITUTION SCHEME

BRANCH
PORT ORCHARD, WA
DEPOSIT DATE
JANUARY 15, 1988
ACCOUNT NAME
TREASURER'S OFFICE

	DOLLARS	CENTS
CURRENCY	1,000	00
COIN		
CHECKS LIST BY BANK NUMBER (EXAMPLE: 19-2)		
18-4 MARY M. SMITH	1,000	00
16-2 SUE A. JAMES	1,000	00
TOTAL	3,000	00

1 SEATTLE-FIRST NATIONAL BANK

ACCOUNT NO. 1111 — 101701
☒ CASH ☐ CHECK
RECEIVED OF JOHN A. JONES
ADDRESS 1500 MAIN STREET

DETAIL	ACCOUNT	NOTE
AMOUNT DUE	1,000.00	
AMOUNT PAID	1,000.00	
BALANCE DUE	-0-	

818-1

ACCOUNT NO. 2222 — 101702
☒ CASH ☐ CHECK
RECEIVED OF SAM E. ADAMS
ADDRESS 1400 ELM STREET

DETAIL	ACCOUNT	NOTE
AMOUNT DUE	1,000.00	
AMOUNT PAID	1,000.00	
BALANCE DUE	-0-	

818-1

ACCOUNT NO. 3333 — 101703
☐ CASH ☒ CHECK
RECEIVED OF MARY M. SMITH
ADDRESS 1200 MAPLE DRIVE

DETAIL	ACCOUNT	NOTE
AMOUNT DUE	1,000.00	
AMOUNT PAID	1,000.00	
BALANCE DUE	-0-	

818-1

LAPPING SCHEME

A lapping scheme can be perpetrated in any cash receipting activity; but, it's most often associated with an accounts receivable function. This scheme is perpetrated by a cashier or accounting clerk who issues cash receipt forms for customer payments, but subsequently makes no bank deposit, or a short bank deposit, of the funds. The difference between the total amount receipted and the lesser amount deposited is stolen (borrowed). Cumulative cash shortages over a period of time represent the total amount of the loss in a lapping scheme. The customer's account for each unrecorded transaction is always marked "paid".

Lapping schemes are perpetrated at decentralized cash receipting locations where funds are initially received from customers, and at the central treasury function after funds have been transmitted there for subsequent deposit in the bank. This type of cash receipts fraud is not very smart (i.e.; dumb), because the inevitable day of reckoning comes when the perpetrator realizes that the lapped amount must be disposed of in some manner before they are detected.

Types of lapping schemes.

> Simple. While all cash receipt transactions are receipted by the cashier each day, funds received on a subsequent date are used to cover the initial shortage. The cumulative amount of the loss is systematically rolled through the accounts.
>
> Complex. Cash receipt forms are not necessarily issued for all customers payments, such as for checks received through the mail. Funds received today are first stolen. Then, funds received on a subsequent date are used when cash receipt forms are issued covering the amount of the previously omitted transactions. Funds received from customer "B" are credited to the account of customer "A". The perpetrator must keep an accurate record of the transactions which have not been recorded (or have been inaccurately recorded) in the accounting records because the cashier or accounting clerk must post payments to these accounts in a sufficient amount of time to prevent customer feedback from delinquent billing notices.

Ways perpetrators conceal the disposition of lapping schemes:

- Make restitution or pay back the amount of the loss, either secretly or by informing the entity.
- Cancel the accountability established by the cash receipts issued, such as by unauthorized voiding activity.
- Destroy the supporting documents representing the accountability for the funds stolen.
- Reporting a mysterious disappearance theft of cash receipts.

Ways to provide audit coverage to all entity funds:

- Prepare an inventory of all decentralized cash receipting functions from a review of revenue reports, cash receipt forms at the central treasurer function, and from discussion with knowledgeable employees.

- Prepare an inventory of all imprest and change funds by purpose, amount, custodian, date, and location.

- Audit all local revenue sources on a cycle (at least once every 3 years).

    - Use comparative analytical reviews to determine which functions have unfavorable trends.

    - Determine reason(s) why revenue changed from previous reporting periods.

    - Confirm responses obtained from managers by using alternative records or through substantive audit tests.

    - Perform unannounced cash counts. Accountability includes the authorized amount of the imprest or change fund, if any, plus all cash receipts issued since the last turn-in to the central treasury function.

    - If fraud symptoms are present, protect the accounting records from loss.

Red Flags:

- Inappropriate employee segregation of duties.

- Deposit timing lags from decentralized locations to the central treasurer function.

- Deposits are not made daily or intact.

- There is an excessive amount of "void" cash receipt transactions.

- The check and cash composition of the bank deposit does not agree with the check and cash composition of the cash receipts issued (i.e.; less cash and more checks).

- A mysterious disappearance theft of cash receipts is reported, particularly at decentralized cash receipting locations.

- Official prenumbered cash receipt forms are not turned-in in numerical order, or are missing.

Fraud Detection:

- Review the segregation of duties of key personnel.
- Review the timeliness of deposits from decentralized locations to the central treasurer function.
- Review the check and cash composition of daily bank deposits during unannounced cash counts and in substantive cash receipts tests.
- Observe cash receipting operations when visiting decentralized locations.

CASE EXAMPLES

An accounting clerk in a county alcoholism program, a decentralized cash receipting location, stole $17,800 from user fees collected from clients. A relief clerk detected the fraud when the perpetrator went on maternity leave. Lapped cash receipt transactions were delayed almost 4 months (i.e.; cash collected in May was used to make the deposit covering cash receipts which had been written in January).

A relief cashier in a county district court stole $9,100 from customer traffic citation payments. Accountability for traffic citations was not entered on the computer when cash payments were made. All documents (i.e.; traffic citations and cash receipts) were taken home. Partial restitution (lapping) was accomplished by making delayed payments on these accounts ($2,500). There were two different frauds operating in this court at the same time, with each cashier acting independently and without the knowledge of the other. This lapping scheme was detected while court personnel were researching records associated with the other fraud.

An accounting clerk in a county district court probation department stole $1,700 from client fees. When transactions were received from decentralized court locations, only a portion of the funds were receipted and deposited. The remainder of the funds were subsequently receipted at a later date (i.e.; borrowing). This fraud was detected by an unannounced cash count during a routine audit. Transmittal documents in the possession of the clerk established accountability for the funds which were not available at the time of the audit.

ACCOUNTS RECEIVABLE SCHEMES

Accounts Receivable Control Account. Although this account is used to maintain integrity of the data recorded in the organization's accounting system, many small entities don't have one. When this happens, we can determine the mathematical accuracy and total amount of the account balances recorded on subsidiary ledger cards or other records. These records can be maintained either in a manual file or on computers. However, the problem is that no one can determine whether the total amount of all the individual account balances represents the correct accounts receivable amount that should be reported on the organization's financial statements. The

attribute of "completeness" causes us to ask one primary question: What's the universe of all account balances in the system?

When small entities don't maintain an accounts receivable control account, we recommend that managers maintain a document that includes data on the summary totals for all customer account balances. For each accounting period, this includes: (a) the beginning balance of all accounts; (b) all new billings for services; (c) all revenue collected from customers; (d) all adjustments and write-offs of account balances; and, (e) the ending balance. This record easily can be maintained on a single manual ledger card or in a similar computer record. This document makes it easier to answer that nagging question we asked in the previous paragraph: What's the universe?

Cashiers and accounting clerks (and their supervisors) who use accounts receivable schemes to defraud employers must continually manipulate the entity's accounting records in order to conceal the loss from managers, customers, and auditors. While most accounts receivable schemes require hard work by the perpetrator, they're easy for auditors and managers to understand (i.e.; not complex).

Types of Fraud Schemes. Manipulations in "on-book" accounts receivable frauds include at least the following types of schemes:

- Check for Cash Substitution Schemes.

  Perpetrators steal unrecorded checks from non-accounts receivable revenue streams (i.e., miscellaneous revenues or one-time charges) and exchange them for cash in an equal amount from accounts receivable transactions that have been recorded in the accounting system. When this occurs, the check and cash composition of the bank deposit will not agree with the mode of payment (i.e.; check or cash) of all cash receipt transactions for each business day. The cash is simply stolen.

- Lapping Schemes.

  In this most common scheme in the accounts receivable function, a perpetrator first steals customer A's payment and then applies customer B's payment to customer A's account balance. To prevent managers and customers from discovering these manipulations, the fraudster must keep accurate records of all accounts involved in the scheme. These records normally are maintained somewhere in the employee's office or desk. The perpetrator rationalizes that the money is only being borrowed and intends to make full restitution later. But, as the size of the scheme increases over time, employees soon realizes that it will be impossible to replace the money. They stop keeping records, but must ensure that all manipulated accounts have been properly credited by the end of the billing cycle. This is a stressful juggling act that often requires the fraudster to come to work early and stay late. They need this quiet time to conceal the scheme from managers and be present in the workplace to respond to any customer complaints. One of their biggest fears is being absent from the workplace because that's when the risk of detection is highest. We're always thankful for the inevitable family emergency that comes along because many accounts receivable schemes are uncovered when another employee performs the fraudster's job and discovers the irregularities. Eventually, the perpetrator can't manage the scheme because of the amount of the loss and the number of accounts they're manipulating. The scheme begins

to unravel, and this is when mistakes are made. To avoid this, fraud perpetrators often conceal losses in delinquent or slow-pay accounts.

- Other Accounting Manipulations.

A perpetrator manipulates accounting records by recording a smaller amount of cash receipts in the control account (which agrees with the daily bank deposit total) than is recorded on the subsidiary ledger cards for all customer payments. This causes an imbalanced condition between the control account balance and the total of the balances on all subsidiary ledger cards. We receive frequent inquiries from financial managers who want to know how an employee could possibly record different amounts in these records. This is a one-sided transaction, that's for sure. Many times managers or auditors discover these conditions and simply write-down the control account balance by using unsupported adjustments to make it agree with the total of the subsidiary account balances. They do this because they just can't seem to find a reasonable explanation for this unusual condition. However, these adjustments simply eliminate the accountability for any missing funds. These adjustments are only made when no one has been able to detect a fraud that's in progress. If someone detects a fraud, the managers or auditors obviously would take different actions.

These unsupported adjustments eliminate accountability for the missing funds and help to mask or conceal the scheme for long periods of time. Some say their organization's computers will prevent this from happening. But it's still possible to perpetrate these fraud schemes without detection. Often, managers are so trusting that they fail to monitor the critical accounting reports that clearly show what's happening within their operations. in another column in this series.

- Eliminating Customer Accounts.

In certain entities, such as those that provide utilities, a dishonest employee in the accounts receivable function can disregard the debts of some customers. These can include the fraudster's own account or those of their relatives or other employees who are their friends. The employee may eliminate the accounts from the accounts receivable billing system or store the subsidiary ledger cards for those accounts in a separate file. These off-line accounts are never billed by the organization. Thus, services are "free". In a utility, the customer books are the original source documents that prove the universe of all accounts in existence. In other organizations, the master list of all credit cards issued to customers serves the same purpose.

When dealing with this type of fraud in the past, our major focus was on the employees who performed the computer input function after the utility meters were read and documented by other employees. But, we've now shifted this focus to others in the organization because many utilities are using hand-held equipment that electronically uploads meter readings directly into the computer. This helps prevent fraud in the input process. However, stubborn fraudsters simply find new ways to do business.

- Fictitious Account Adjustments.

Legitimate account adjustments in accounts receivable include: (a) pre-billing adjustments for unusual circumstances, such as meter reading errors and broken transmission lines or facilities; and, (b) post-billing adjustments for other miscellaneous accounting errors noted by both employees and customers for a wide variety of reasons. Account adjustments in delinquent accounts usually totally eliminate a debt.

However, unsupported account adjustments simply eliminate the accountability for money from real debts owed to the organization after customer payments have been stolen. These adjustments represent a high risk for fraud, similar to any other kind of negative cash transaction. All computer accounting systems should, but don't always, produce exception reports that identify the universe of the customer account adjustments processed each business day. And, even if such reports are produced, managers often don't adequately monitor these high-risk operations. Account adjustment fraud schemes aren't always perfect, but they do represent some of the more memorable cases we've ever encountered.

- Stealing the Statements.

Some perpetrators who steal customer payments don't have the ability to write-off account balances. Thus, these employees are forced to resort to "stealing the statements" of customers with invalid delinquent account balances to conceal that they've misappropriated the funds from the payments made by these customers. They do this inside the organization before the statements are mailed and outside the organization after the statements have been mailed. In both scenarios, customers receive manually prepared statements indicating that they owe only amounts due from charges in the current billing period. The fraud perpetrator must then conceal the delinquent account balances from managers and customers.

These schemes are almost always doomed to failure because eventually the organization is going to send a delinquency notice to a customer who responds by saying, "My account isn't delinquent, I paid my bill." They then produce cash receipts or canceled checks to prove this condition. An independent customer service department must carefully listen to customer complaints and research each problem thoroughly. If a cashier or accounting clerk who manipulated the account is also responsible for responding to these inquiries, they often tell customers that the organization is experiencing computer problems. They then make fictitious account adjustments that conceal the irregular activity. This enables them to correct their mistakes and keep the scheme active for long periods of time. These schemes are often complex and very interesting.

Method of Documenting Accounts Receivable Losses. Once fraud has been detected in the accounts receivable function, we make sure that the organization separates the suspect employee from the accounting records. Most employees simply are placed on administrative leave while the fraud investigation is conducted so that they can't continue to manipulate the accounting records. We just let the computer send out customer statements without any outside intervention.

We use computerized billing statements, depicting all balances owed by customers, as the most common method to determine the total amount of the loss in an accounts receivable scheme. Customers' complaints about irregularities identify the universe of all manipulated accounts. We ask the organization to maintain a master log of all complaints and resolutions after it

compares customers' records of account payments to information in the computer system. The entity must obtain copies of supporting documents from customers for any unrecorded payments. These supporting documents must be maintained on file to support any account adjustments and for audit purposes. We then verify the accuracy of this tabulation.

Summary of Major Areas of Concern in Accounts Receivable Systems

The main issue in a utility accounts receivable fraud case is that someone in a utility operation is going to **steal cash receipts** (currency or checks). Once this is done, the employee will do whatever they are able to do (i.e.; what they are able to control) to keep the fraud from being detected by management or auditors. For example:

Problem: When employees steal a customer's payment, they have to make the account "right" or suffer the resulting **customer feedback**. The employee must do one of two things in order to conceal the irregular activity. They either **write-off the account**, such as through a "non-cash credit" transaction (i.e.; an account write-off, adjustment, or cancellation), **or let the account go delinquent** (i.e.; without taking any action). This latter condition is very dangerous and usually results in customer feedback and detection of the scheme. It's extremely important for all customer feedback to come to an **independent party or function** for proper research. Customer feedback should not come back to the accounts receivable function where a dishonest employee will further manipulate the records to conceal any irregular activity from view by managers.

Solution: Management reviews and audit tests in utility accounts receivable operations must focus on these two alternatives available to cashiers. The accounts receivable accounting system should produce an "exception" report at the end of each business day listing the universe of all "non-cash credit" transactions. Each transaction should be authorized and approved, and be supported by appropriate documentation for the action. Delinquent accounts should also be monitored closely. Customer account confirmations should be considered.

The next **most common attribute** auditors see in utility accounts receivable fraud cases is that the total amount of customer payments is **more than** the total amount of the bank deposits. Therefore, we should always perform this test. And, an independent party from cashiering and account maintenance should routinely reconcile this information.

When accounts are written-off, we need to review the **exception report** that lists the universe of all such transactions to determine whether all write-offs have been authorized and approved as well as properly supported. Typically, employees have no support for fictitious write-off transactions. We often forget that employees who have the ability to process such transactions **always** have the ability to do this 24 hours a day, 7 days a week, 365 days a year, whether it's authorized or not. Therefore, the "exception" report is mandatory for use as a monitoring tool in the accounts receivable system.

For delinquent accounts, we should **confirm** significant outstanding account balances with customers. But, when fraud is involved, why doesn't the customer know? The answer to that

question is that an entity employee has purposefully suppressed this information from view. Customers are placed on **"no bill"** status or are receiving manual bills from the utility showing charges from only the current period (**stealing the statements**). We should review the computer list of all accounts not billed to ensure that the justification for each such account is appropriate. We should also review the computer list of all accounts scheduled for **"shut-off"** to ensure that customer services were terminated as required by law.

Knowing what **miscellaneous revenue streams** exist at the utility is also extremely important. These revenue streams are the **primary targets** of cashiers because there often are few accounting records that help anyone identify the universe of these transactions. In addition, the cash receipting systems that exist to account for and document these revenues are often deficient.

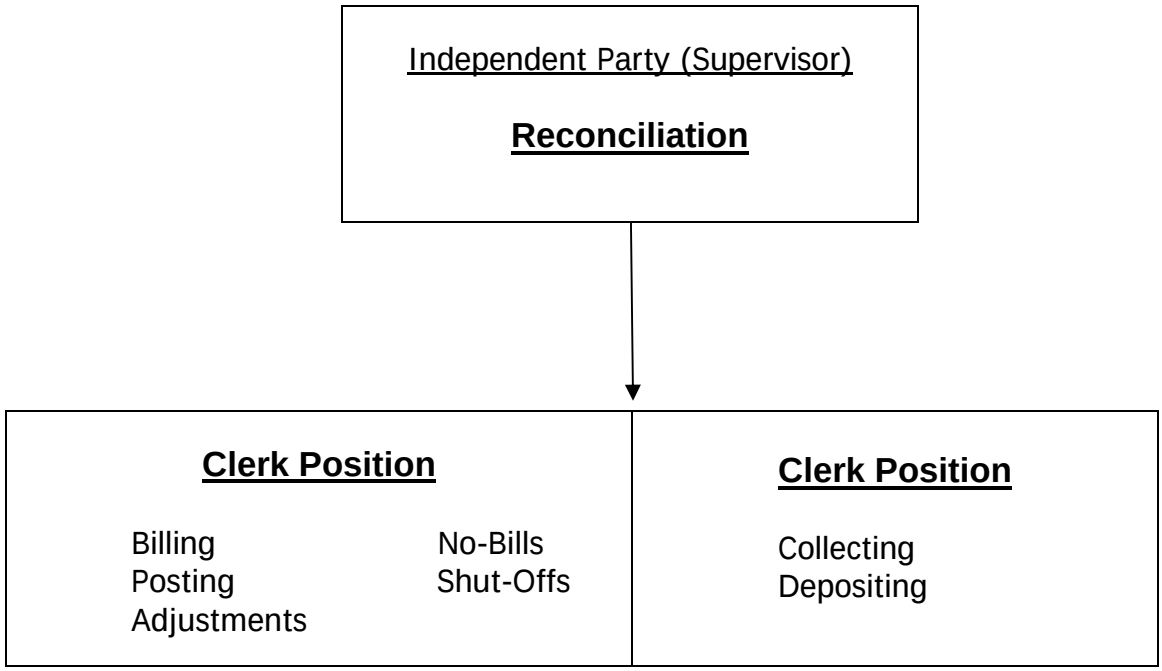
In addition, we should always review the amount of **cash in utility bank deposits** to determine if it is reasonable based upon the collective knowledge of managers and auditors. When frauds occur, cash is conspicuously **missing** from the bank deposits.

Accounts Receivable – Internal Control Structure - Duties of Personnel

The ideal separation of duties for employees working in the accounts receivable function is as depicted in the diagram shown below. Three employees are needed. But, this is not always possible. Therefore:

If one person performs all duties in the function, someone independent of the employee must monitor their work.

If two employees perform all duties in the function, their duties should be split between billing and posting the accounting records and collecting and depositing funds. But, someone independent must perform the reconciliation of account postings and bank deposits. If this is not possible, the employee performing the billing and posting duties should also perform the reconciliation (least risk) rather than the employee collecting and depositing funds (highest risk).



Red Flags:

- Inappropriate employee segregation of duties.
- Deposits are not made daily or intact.
- The check and cash composition of the bank deposit does not agree with the check and cash composition of the cash receipts issued (i.e.; less cash and more checks).
- The entity does not maintain an accounts receivable control account.
- The balance in the accounts receivable control account does not agree with the total of the customer account balances recorded on the subsidiary ledger cards.
- Total credits to subsidiary ledger cards do not agree with total bank deposits in the same accounting period.
- Total customer books or the total of all credit cards issued to customers do not agree with the total of all subsidiary ledger cards or accounts in the file.
- The entity receives customer feedback involving transactions from accounts receivable systems through:

(a) Cashiers or individuals who record payment information on customer subsidiary ledger cards or in similar computer records for customers in the accounting system; or,

(b) A customer service unit where employees perform this review in a perfunctory manner, or aren't properly trained to identify transaction attributes which might be fraud.

- Managers don't have an aggressive collection program for delinquent balances in accounts receivable accounts, or the amount of delinquent accounts receivable has been increasing over time.

- Managers don't produce an exception report identifying high-risk transactions, such as cancellations and adjustments of account balances in accounts receivable accounts, and transactions aren't authorized by someone who is independent of the function or supported by adequate documentation.

Fraud Detection When Control Accounts Are Maintained:

- Review the segregation of duties of key personnel.

- Review the check and cash composition of daily bank deposits during unannounced cash counts and during substantive audit tests of cash receipts.

- Steps to detect fraud schemes in an accounts receivable function when control accounts are maintained include the following:

  Step Number 1. As of a specific cut-off date, agree (compare) the balance in the accounts receivable control account to the total of the customer account balances recorded on the subsidiary ledger cards in the file.

  Step Number 2. For a specified accounting period (i.e.; day, week, month, or year), agree (compare) the total of all credits recorded on the subsidiary ledger cards in the file to the: (a) total cash collections posted to the control account; (b) total bank deposits; and, (c) total cash receipt forms issued or total collection stubs on file, depending upon the accounting system used. When comparing total credits to customer accounts to related bank deposits and using this as an analytical procedure, remember that this is also a substantive audit test. Deposit shortages represent losses of funds.

  Step Number 3. Where possible, such as in a utility accounts receivable system (i.e.; water, sewer, electricity, garbage, etc.), agree (compare) the total number of all customer books (i.e.; meter, route, location, etc.) to the total number of active subsidiary ledger cards in the file or active customer accounts on a computer system. Think universe. Review the propriety of all customer accounts included on a "no bill" report. Determine if the entity ensures that all new accounts (e.g.;

meters) are effectively communicated to utility billings. In a customer credit card system, agree (compare) the total number of credit cards issued to the total number of subsidiary ledger cards in the file.

Step Number 4. Review accounts receivable credits (i.e.; cancellations and adjustments), with emphasis on transactions which affect the accounts of employees and their relatives, and transactions that affect only the control account. Review customer accounts receivable write-offs for propriety. Determine if the entity has an exception report listing the universe of these high risk transactions, and whether all adjustments are approved and properly supported. Again, think universe.

Step Number 5. As of a specific cut-off date, confirm all delinquent customer accounts receivable balances if significant or warranted. When irregularities occur, employees sometimes divert customer billing statements to themselves, such as by changing the mailing address to their own address or to a post office box they control. Sometimes delinquent accounts balances are manipulated and billing statements sent to customers showing no balance due from prior periods. These irregularities are called "stealing the statements".

Step Number 6. Review billing rates for propriety. Analyze all flat (standard) fee or rate customer accounts. Test actual billing rates to the authorized billing rate established by resolution, ordinance, or other authorized rate structure.

Step Number 7. Determine whether the entity knows the percentage of their customer payments that are made in cash, and whether this expectation is being met. Determine if there is any (or a sufficient amount of) cash in the daily bank deposits.

CASE EXAMPLES

An elected county treasurer stole $62,400 over a three year period from property tax receipts. After cash receipt transactions were batched and posted to both accounting records and tax roll records by office employees, the treasurer altered cash receipt records to reduce the amount of accountability for cash every other business day. The total of all cash receipt documents in each batch did not equal the total amount shown in cash receipt records. However, the amount of the bank deposit equaled the cash receipt records (summary level document), and agreed with the amount posted to the taxes receivable control account. Since all transactions in each cash receipts batch were posted to the tax roll (accounts receivable subsidiary ledger cards), this created an imbalance condition between the control account and the subsidiary records. The taxes receivable control account was arbitrarily written-off (down) every three years in an amount about equal to the loss shown above. While there was no support for this adjustment, the treasurer periodically wrote-off the amount of funds stolen. When mode of payment information was reviewed on the days when losses occurred, the amount of the shortage reflected in each batch of cash receipts also agreed to the amount of cash that was missing (in composition) from

office records indicating the treasurer's total cash accountability for each day. For example, total cash at end of day yesterday, plus all cash receipt transactions today, did not equal the total cash at the end of today. The difference represented the exact amount of funds deleted from accountability when the summary cash receipt records in the office were altered that day.

A utility district cashier stole $900 from customer water payments in an accounts receivable environment. This case involved a check for cash substitution scheme to initially convert the funds for personal gain (borrowing), a lapping scheme because the accounts were subsequently paid by the cashier at a later date, and a manipulation of accounts receivable records (the loss was temporarily concealed in customer slow-pay account balances). The cashier could not permit any account to be reported in a delinquent status because of the district's policy of terminating water service to such customers. If this had happened, the customers would have been able to produce a copy of their "paid" billing stub and their cancelled checks to prove that their account had been paid. When these funds were initially stolen, the cashier retained the district's copy of the customer's billing stub so that a record could be kept of all accounts (and amounts) manipulated. When repayments were made before the next billing cycle occurred for these customers, the cashier entered the billing stub into accountability and made a cash (i.e.; currency) payment on the account. The district manager helped this cashier balance her account one day and detected the check for cash substitution scheme (one transaction for a minor amount). The cashier confessed and promised never to borrow funds again. The district retained this individual in a cashier position (no subsequent bond coverage). The perpetrator continued to steal money by manipulating only cash payments since these transactions could not be easily detected by management. When fired for another reason, the cashier continued to make repayments (in hopes that the scheme would not be detected). This individual included the billing stub and a money order payment in envelopes with the return addresses of the customers whose accounts had been manipulated. While the district rarely received money order payments, money orders mysteriously appeared in large numbers after this cashier left (suspicious activity). For example, all 10 money orders received in a single day were sequentially numbered from the same source (one convenience store). It was unlikely that these 10 customers all stood in line at a single source to purchase money orders to pay their water bills. The cashier confessed.

An office assistant in a water district and a city water utility cashier stole $1,400 and $1,900, respectively, from customer water payments in an accounts receivable environment. These losses were concealed in delinquent accounts receivable balances. In the first case, payments were recorded as credits in accounts other than the account of the customer making the payment (complex accounting records required by perpetrator). In the second case, the loss was detected before repayment could be made. A relief cashier detected the loss when the primary cashier went to the dentist. The entire change fund was also missing. In addition, billing stubs were on-hand, but there were no corresponding funds on-hand (cash shortage).

Fraud Detection When Control Accounts Are Not Maintained:

- Review the segregation of duties of key personnel.

- Review the check and cash composition of daily bank deposits during unannounced cash counts and during substantive audit tests of cash receipts.

- Steps to detect fraud schemes under these circumstances are as follows:

  Step Number 1. Determine whether the entity maintains an accounts receivable control account. Auditors may disclaim an audit opinion on accounts receivable reported in the entity's financial statements. However, the recommended approach is to perform substantive audit tests of cash receipts to determine the accuracy of the account balance and the effect, if any, of this internal control weakness.

  Step Number 2. For a specified accounting period (i.e.; day, week, month, or year), agree (compare) the total of all credits recorded on the subsidiary ledger cards in the file to the: (a) total bank deposits; and, (b) total cash receipt forms issued or total collection stubs on file, depending upon the accounting system used. When comparing total credits to customer accounts to related bank deposits and using this as an analytical procedure, remember that this is also a substantive audit test. Deposit shortages represent losses of funds.

  Steps Number 3 Through 7. Same as indicated above when control accounts are maintained.

There are two methods used to misappropriate funds when the entity does not maintain an accounts receivable control account.

One Person Operation. There is a segregation of duties problem because the same person bills all customers, acts as cashier for all cash collections, makes the bank deposit, and posts all payments to the subsidiary ledger cards.

After customer payments have been made, the cashier: (a) marks the customer's account "paid"; (b) fails to issue a cash receipt form, if used, or destroys the entity copy of the payment document (i.e.; utility stub or receipt); and, (c) steals an amount of money equal to the amount indicated on the documents which have been destroyed. After these actions are taken, the following conditions exist:

The total of all cash receipt forms or utility billing stubs retained on file always equals the amount of the bank deposit.

Credits posted to the subsidiary ledger cards for each customer for any business day, or total credits posted to all subsidiary ledger cards for a period of time: (a) do not equal the total of the related bank deposits; and, (b) do not equal the total of the related cash receipt forms or utility billing stubs retained on file.

Fraud Detection:

- Agree (compare) the total of all subsidiary ledger card postings for a period of time to the amount of the related bank deposits and the cash receipt forms or utility billing stub batch totals during this same period.

- Fraud is not detected when these audit tests are performed:

    - Verify the mathematical accuracy of the total of all cash receipt forms or utility billing stubs retained on file.

    - Agree (compare) the total of all cash receipt forms or utility billing stubs retained on file to the related bank deposits.

    - Agree (compare) all payments indicated on the cash receipt forms or utility billing stubs retained on file to the credits posted to the individual subsidiary ledger cards (backwards audit test).

Fraud In A One Person Operation

	Billing Stubs	Deposit	Subsidiary Ledger Cards	
	X-1		X-1	X-6
	X-2		X-2	X-7
	X-3		X-3	X-8
	X-4		X-4	X-9
	X-5		X-5	X-10
Totals:	5	5	10	

Two Person Operation. There is an adequate segregation of duties in the entity where one person bills all customers and posts all payments to the subsidiary ledger cards, while the other person acts as the cashier for all cash collections and makes daily bank deposits. The cashier always manipulates cash receipt records and dupes the second individual into posting all accounts "paid" even though funds have been stolen.

After customer payments have been made, the cashier: (a) prepares an adding machine tape which indicates a reduced amount of cash accountability for the day and wraps it around the daily batch of cash receipt forms or utility billing stubs; (b) makes the daily bank deposit which agrees with this altered adding machine tape total (but does not equal the total of all cash receipt forms or utility billing stubs included in the batch); (c) steals an amount of money equal to the amount that the daily bank deposit and batch of cash receipt forms or utility billing stubs have been reduced; and, (d) transfers the batch of utility billing stubs to the individual who posts the credits to the subsidiary ledger cards. This individual removes the adding machine tape and

ignores it (because it isn't needed to perform this function), and then proceeds to mark all customer accounts "paid" on the subsidiary ledger cards (total credits posted equal the total of all cash receipt forms or utility billing stubs in the batch, but do not equal the amount of the bank deposit). After these actions are taken, the following conditions exist:

- The total of all cash receipt forms or utility billing stubs retained on file does not equal the total indicated on the adding machine tape attached to the batch or the amount of the bank deposit.

- Credits posted to the subsidiary ledger cards for each customer for any specific day, or total credits posted to all subsidiary ledger cards for a period of time, do not equal the total of the bank deposit for that date or period.

Fraud Detection:

- Verify the mathematical accuracy of the total of all cash receipt forms or utility billing stubs in each daily batch and agree (compare) it to the total of the tape attached to the batch and to the total of the daily bank deposit. Anyone with a calculator can detect this fraud. (NOTE: Use bank validated deposit slips or bank deposit information from the bank statement for this audit test, not a duplicate copy of the deposit slip document retained on file, because perpetrators often prepare two deposit slips: (a) one for the reduced bank deposit amount which is retained on file; and, (b) another for the actual deposit amount which goes to the bank, but which isn't retained on file.)

- Agree (compare) the total of all subsidiary ledger postings for a period of time to the amount of the bank deposits (and the cash receipt forms or utility billing stub batch totals) during this same period.

- Fraud is not detected when this audit test is performed:

  Agree (compare) all payments indicated on the cash receipt forms or utility billing stubs retained on file to the credits posted to the individual subsidiary ledger cards (backwards audit test).

Fraud In A Two Person Operation

	Billing Stubs		Deposit	Subsidiary Ledger Cards	
	X-1	X-6		X-1	X-6
	X-2	X-7		X-2	X-7
	X-3	X-8		X-3	X-8
	X-4	X-9		X-4	X-9
	X-5	X-10	_____	X-5	X-10
Total Stubs	10			10	
Total Tape	5		5		

CASE EXAMPLES

One Person Operation.

A recording clerk in the auditor's office stole $1,400 from user fees collected from state agencies for officially recording documents in the county's records. Documents were recorded on a credit basis, and state agencies paid the amount due monthly. A check for cash substitution scheme was used to convert state agency warrants to cash when the individual was a relief cashier. There was no control account over this miscellaneous accounts receivable function in the recording section. The recording clerk borrowed cash at the end of one business day (i.e.; temporary short deposit), but did not return to work the following day because of a child's illness. The cash shortage was detected by another cashier who assumed her duties. An analysis of all other tasks performed by this clerk detected the fraud.

Two city water utility cashiers stole $6,700 and $8,600, respectively, from customer payments in an accounts receivable environment. A check for cash substitution scheme was initially used to misappropriate funds. These entities did not maintain accounts receivable control accounts. These cashiers destroyed certain utility billing stubs, marked all customer accounts "paid", and stole an amount of funds equal to the manipulated transactions.

A city water utility cashier stole $7,300 from customer payments in a computer accounts receivable environment. The cashier eliminated utility billings for herself and other family members from the computer system (i.e.; unsupported and unapproved credit adjustments to these accounts). However, the bulk of this loss came from other cash receipts. The cashier first identified a group of customers who made their monthly payments in cash (i.e.; currency). Unknowingly, 25 city water utility customers became the personal clients of this cashier. These customers were removed from the computer system by using the computer pre-bill adjustment mechanism. Each such customer was sent a flat fee bill (minimum service charge) during each subsequent billing cycle. The cashier prepared manual bills for these customers. The city paid the postage fees for these customer billings (i.e.; sent out at the same time as other utility billing documents). When these customers paid their bills, the cashier destroyed the billing documents and stole the funds from these transactions. Once deleted from the computer system, further water usage by these customers was not posted from the meter books to computer accounts receivable records. All computer billing and collection history records for these customers were blank.

A city water utility cashier stole $16,900 from customer payments in a computer accounts receivable environment (one year fraud, because all prior city records had been destroyed by this 17-year employee). The cashier first processed all check payments on the computer system, and then prepared a sub-total daily activity report (cash receipts journal). This sub-total report looked exactly the same as the total report (i.e.; same name, etc.), except that the number shown on the report was different (hard to distinguish). The cashier used this sub-total report to make cash receipt turn-ins to the central treasurer function where these revenues were again receipted into accountability and included in the daily bank deposit. The cashier then processed all cash payments on the computer system, and prepared the total daily activity report. This report was then destroyed, and all funds represented by the cash payments were stolen. When the total

computer report was produced, all customers accounts were marked "paid". The city hired a consultant to study the water utility prior to the audit which could have detected this fraud scheme (but didn't). The consultant reported that the utility was losing about $17,000 a year, but didn't give the city a clue as to why (probably compared total subsidiary ledger card credits in the system to total cash receipts to establish the amount of this loss). Since the city didn't know what to do with the study, they simply disregarded it. Although not aware of the utility study until after the audit was completed, auditors proved this condition did exist.

Two Person Operation.

A city water utility cashier stole $21,500 from customer payments in an accounts receivable environment. A check for cash substitution scheme was initially used to misappropriate funds. This entity did not maintain an accounts receivable control account. There were two individuals assigned to the water utility function. This fraud was perpetrated exactly as described in the narrative above (i.e.; the cashier manipulated cash receipt records and duped the second individual into posting all accounts "paid" even though the funds were stolen).

ACCOUNTS RECEIVABLE FRAUD CASES

January 1, 1987 Through December 31, 2001 (**15 Years**)

Amount	Description
$ 2,819	Asotin County - Sewer Fund (2001). A Receptionist/Bookkeeper took recorded cash receipts from revenues of three County Departments, including the Sewer Fund. As a result, bank deposits were less than recorded accountability for funds collected (cash shortages). Accounting records were falsified in an attempt to conceal these activities. There was an inadequate segregation of duties for this employee who acted as a cashier, made bank deposits, and then reconciled the amount of revenue collected with actual bank deposits. The County did not adequately monitor this individual's work. **The issue**: Customer credits more than bank deposits.
19,827	City of Kelso – Water Utility (2001). A Utility Billing Clerk took cash receipts from 137 customers making payments on delinquent accounts. To conceal these cash shortages and account irregularities, the employee manipulated the computer information in the customer's account to delete any delinquent amounts when the utility bills were subsequently prepared. The employee then prepared billing statements that showed only the current amount owed and mailed them to the customers (stealing the statements). After printing the false customer billing statements, the employee reentered the deleted computer information to ensure the utility subsidiary ledger reconciled with the City's general ledger. The employee also manually altered computer reports listing all delinquent accounts to prevent the City from sending delinquency notices to the affected customers and to stop their utilities from being shut off. There was an inadequate segregation of duties for this employee who was responsible for posting payments to customer accounts, billing customers, reconciling delinquent utility accounts,

and shutting off utilities on unpaid accounts. The employee also acted as a relief cashier, and the City did not adequately monitor this individual's work.

The issues: (1) Delinquent accounts (due to lack of write-off authority). (2) Stealing the statements via internal computer manipulations of the affected accounts.

337 Silverdale Water District (2001). A cashier took currency from one customer utility payment and then processed a fictitious write-off to eliminate the account balance and conceal the irregular activity. We selected transactions with similar characteristics for confirmation with the taxpayers. This investigation subsequently identified a total of six transactions with these attributes.

The issue: Fictitious write-offs (think universe and exception report).

1,381 King County Water District No. 54 (2001). An Office Manager deposited customer utility payments into the District's petty cash checking account, taking "cash back" ($71) from one deposit, and then issued four checks made payable to "cash" or to himself ($701). The signature of the District Superintendent was forged on these checks. Fifteen customer payments were not posted to accounts receivable accounts or deposited in the bank ($516). Ten of these customer payment stubs were in the Office Manager's possession. Three accounts were written-off and not approved by the Board ($93).

The issues: (1) Fictitious write-offs (think universe and exception report). (2) Delinquent accounts.

131 King County Water District No. 111 (1999). A cashier took cash receipts from two over-the-counter customer payments. Detected by customer feedback.

The issue: Delinquent accounts (due to lack of write-off authority).

3,088 City of Yakima (1999). Cashier took utility payments from 30 customers in a two-month period. Detected by customer feedback.

The Issue: Delinquent accounts (due to lack of write-off authority).

7,315 City of Sultan (1999). Deputy Clerk-Treasurer took customer utility payments made in cash at City Hall. These transactions were not receipted into the computer system, but were posted to the utility accounts using a restricted computer screen. Customer accounts were kept current and delinquent accounts did not show on the customer's next billing.

The issue: Fictitious write-offs (think universe and exception report).

$ 36,774 City of Battle Ground (1997). Utility clerk took currency from utility cash receipts. Transactions were first recorded on a cash register (Quadrant) and then interfaced with the accounts receivable computer system (Eden). Cash register

records were then destroyed and transactions re-entered at lower amount eliminating customer payments made in cash. The resulting reduced accountability for funds then agreed with the bank deposit. Accounting records were destroyed. Deposits were not made timely (up to 47 days delay while waiting for computer alterations and account manipulations). Additions funds were taken when customer accounts were also written-off without authorization or approval or supporting documentation.

The issues: (1) Customer credits more than bank deposits. (2) Fictitious write-offs (think universe and exception report). (3) Deposit delays. (4) Transaction number integrity (like cash register "Z" tape number) and time of void/adjustment transactions (late night or weekends). (5) Missing accounting records.

10,730 Belfair Water District (1997). Office manager took cash receipts (currency, money orders, and checks) from utility payments, security deposits, hydrant services, and miscellaneous services for over a year. Additional losses from unrecorded cash transactions were probable, but could not be proved (no accounting records). Condition of accounting records for prior years of utility payments precluded establishing additional losses.

The issues: (1) Customer credits more than bank deposits. (2) System and accounting records show cash payments with no currency in bank deposits. (3) Bank deposit shortages.

298,126 Highline Water District (1997). Accounting clerk operated a lapping scheme for an unknown period of time (see attached case study). Utility cash receipts were stolen, but customer accounts were not marked "paid". Unauthorized "suspense" accounts were created, unauthorized customer account write-offs were processed, and customer feedback went directly to the employee. A check for cash substitution scheme and deposit shortages were the cause of additional losses.

The issues: (1) Aged or delinquent customer accounts (customer feedback must come to an independent party). (2) Fictitious write-offs (think universe and exception report). (3) Identify all suspense accounts in system. (4) Cash count and reconciliation of mode of payment of cash receipts to check and cash composition of the bank deposit. (5) Date of customer payment shown on billing statement as lapping deterrent (slow pay accounts).

90,265 City of South Bend (1994). Clerk/treasurer used a check for cash substitution scheme to misappropriate currency for 7 years. Major missing revenue streams included funds from inter-local government agreements and investment interest. In addition, entire batches of utility payments were stolen after they were recorded in the utility accounting system. The employee also received more pay than authorized.

The issues: (1) Customer credits more than bank deposits (missing deposit batches). (2) Cash count and reconciliation of mode of payment of cash receipts

to check and cash composition of the bank deposit. (3) Identify missing revenue streams(miscellaneous categories).

563,035 City of Walla Walla (1994). Clerk/treasurer stole taxpayer payments from local improvement district (LID) assessments receivable for 8 years using a check for cash substitution scheme involving the city's daily bank deposit. Accounting records were manipulated after other employees balanced the daily deposit. Assessments receivable accounts were not marked "paid" and were shown in the accounting system as delinquent. The computer was not used to bill customers. Instead, manual bills were prepared and mailed so customers would not know the condition of their account.

The issues: (1) Delinquent accounts (think confirmations). (2) Cash count and reconciliation of mode of payment of cash receipts to check and cash composition of the bank deposit. (3) Deposit delays. (4) Foreclosure on property not accomplished. (5) LID computer not used for billing purposes (manual bills prepared indicating current assessment only).

185,409 Kitsap County Treasurer's Office (1993). A revenue officer stole property tax payments using a check for cash substitution scheme involving the treasurer's daily bank deposit. Bank deposit slips were manipulated when the employee was acting as a courier on the way to the bank. Personal property taxes in the advance tax suspense fund were used to pay the taxes for the manipulated customer's accounts. Unrelated personal property tax accounts in the suspense fund were then written-off using a computer software program. Exception reports were not prepared for these tax adjustment transactions (high risk).

The issues: (1) Cash count and reconciliation of mode of payment of cash receipts to check and cash composition of the bank deposit. (2) Fictitious write-offs (think universe and exception report). (3) Missing accounting records.

1,844 City of Bremerton (1991). Utility cashier operated a lapping scheme to steal customer cash receipts and the change fund. Stubs of manipulated accounts were retained in the change fund bank bag. Accounts were not manipulated long enough to go into delinquency status (slow pay accounts).

The issues: (1) Delinquent accounts (due to lack of write-off authority). (2) Date of customer payment shown on billing statement as lapping deterrent (slow pay accounts).

18,443 Town of Rainier (1990). Utility recorded and unrecorded customer cash receipts were stolen by the clerk/treasurer. Unauthorized disbursements were made to self and to vendors for personal items (computer and dishwasher).

The issues: (1) Customer credits more than bank deposits. (2) Bank deposit shortages. (3) Identify missing revenue streams (miscellaneous categories).

7,275 City of White Salmon (1990). Deputy clerk/treasurer billed utility customers manually in lieu of computer billings and took cash payments (her own personal accounts). Some account balances were written-off when utility payments were made and then stolen.

The issues: (1) Fictitious write-offs (think universe and exception report). (2) Agree meter books to total "active" customer accounts in computer system. (3) Utility computer not always used for billing purposes (manual bills prepared about 25 customers indicating current charges only).

900 Skagit Public Utility District No. 1 (1990). Utility cashier operated a lapping scheme to steal customer cash receipts received through the mail. A check for cash substitution scheme and a lapping scheme were used. Manipulated customer accounts were subsequently paid in cash by the employee.

The issues: (1) Delinquent accounts (due to lack of write-off authority). (2) Date of customer payment shown on billing statement as lapping deterrent (slow pay accounts). (3) Cash count and reconciliation of mode of payment of cash receipts to check and cash composition of the bank deposit.

20,782 Town of La Conner (1990). Utility cashier took recorded customer cash receipts and manipulated computer accounts receivable records to show that the accounts had been paid even though the funds were not deposited. Sub-total cash receipts accounting records were retained on file to agree with the bank deposits made with the clerk/treasurer (all check payments). Total cash receipts accounting records indicating that all accounts were marked "paid" were destroyed (cash payments were stolen).

The issues: (1) Customer credits more than bank deposits. (2) Incorrect account reports on file (sub-total versus total).

1,349 Whatcom County Water District No. 12 (1989). Utility cashier took recorded and unrecorded customer cash receipts using a lapping scheme. The cashier entered their own name on the payee line of a check (forgery), and there were petty cash and bank deposit shortages.

The issues: (1) Customer credits more than bank deposits. (2) Bank deposit shortages. (3) Identify missing revenue streams (miscellaneous categories).

8,570 City of Airway Heights (1987). Utility cashier took recorded customer cash receipts (total credits to customer accounts exceeded the bank deposit). There was no accounts receivable control account.

The issues: (1) Customer credits more than bank deposits. (2) No accounts receivable control account (think universe). (3) Agree meter books to total "active" customer accounts in computer system.

696 City of Castle Rock (1987). Utility cashier took recorded customer cash receipts (total credits to customer accounts exceeded the bank deposit). There was no accounts receivable control account.

The issues: (1) Customer credits more than bank deposits. (2) Bank deposit shortages. (3) No accounts receivable control account (think universe).

392 Benton County (1987). Utility cashier took recorded customer cash receipts from the cash drawer (short deposit).

The issues: (1) Customer credits more than bank deposits. (2) Bank deposit shortages.

$ 1,279,488 Totals (22 Cases) – 4.6% of all cases and 14.5% of all dollar losses (**15 years**).

TYPICAL ACCOUNTS RECEIVABLE FRAUD SCENARIO

Warning: Watch out for documents that eliminate the accountability for cash receipts in manual or computer systems (cash registers).

The Fraud: Unauthorized transactions are processed for:

Voids, Paid-outs, and Refunds (Every Organization)
Non-cash credits (Primarily in Courts, but also College Scholarships)
Cancellations (Accounts Receivable Systems-Utilities)
Adjustments (Accounts Receivable Systems-Utilities)
Any Account Write-Off (Accounts Receivable Systems-Utilities)

For every use of these transactions types, there can also be an abuse.

Prevention: Supervisory approval is required for these transaction types.

Use specific forms for these purposes.

Retain all copies of supporting documents on file.

Prepare exception reports for these transactions types.

Review "no bill" and "shut-off" customer account reports.

Monitor the activity of these high risk transactions.

Common Problem: **No (or little) cash** in daily bank deposits.

Does the entity know the percentage of their customer payments that are made in cash? We normally hear everything from 5% to 20% of the total bank deposit/revenue. But one city recently reported the number exceeded 50% because of a change in the population demographics. The question is: What is right for each operation? And, does the entity periodically review their records to see if their expectations are being met?

Does the entity know which customers pay their account in cash? These accounts might also be "flagged" in some way for identification purposes within the entity's computer system. The entity should require **an exception report** of **any adjustments** made to these accounts because they are **the highest risk accounts**. These are the accounts most often manipulated by employees.

Common Failing: Managers often forget that when an employee's job duties include processing adjustments to customer accounts, **this employee always has the ability to process adjustments to customer accounts**, whether these actions are authorized or not. Employees simply process unauthorized adjustments to conceal irregular activity from view. **An exception report is required (think universe)**.

Highline Water District - $298,126 (actual amount was $357,237)

Scheme. Lapping scheme in a utility accounts receivable system. Over 4,000 customer accounts were manipulated until the employee lost control. Cash receipts were stolen; but, customer accounts were not marked "paid". Subsequent payments from other customers were applied to accounts previously manipulated, and so on. Customer feedback went directly to the employee.

Detection. Routine SAO audit in cash receipts testing and review of internal controls for the general ledger and utility billing systems. Discrepancies included: (a) an unauthorized suspense account; (b) billing stubs did not agree with accounts actually posted "paid"; (c) a miscellaneous cash receipt that was never deposited; and, (d) incorrect check and cash composition for the bank deposit from an excess vehicle sale. Of 2,000 account postings and checks in 7 bank deposits, only 1% of the transactions matched.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Segregation of duties problem. One person received funds, posted customer accounts "paid", prepared the deposit, reconciled the depository account bank statement, received customer feedback, and adjusted accounts without supervisory approval. There was no monitoring. She worked early and late, and rarely took vacation. No one ever did her work when she was gone.

(2) The district did not properly control checks which arrived through the mail, and internal controls over cash receipts were practically non-existent (uncontrolled environment).

(3) There was very little cash in bank deposits; but, large cash payments were routinely received at the receptionist/cash receipting function.

(4) Customer feedback was not resolved by an independent party or customer service unit.

(5) Delinquent accounts receivables were not monitored. No aging report was available.

(6) There was a wide variety of irregular documents present in stub batches (also many changes).

Detection Steps.

(1) Review internal controls in accounts receivable operations to ensure proper separation of duties between the billing and posting functions and the cashiering and depositing functions.

(2) Properly perform unannounced cash counts on **all** authorized funds and cash receipts. Analyze the composition of selected bank deposits and scan stub batches for irregularities.

(3) Use six audit steps from Fraud Manual accounts receivable section. Perform analytical procedures of revenue, cash in deposits, delinquent accounts/adjustments, universe of accounts, control and subsidiary account agreement, and agreement of total credits to bank deposits.

Audit Report No. 57983, February 21, 1997. The district is one of the largest public water utilities in the state servicing about 16,500 accounts from Tukwila to Federal Way. The prior audit for Calendar Year 1995 operations included significant internal control weaknesses in the computer accounting system. Unauthorized, undocumented changes can be made to the general ledger master file beginning account balances and the monthly net transaction totals, as well as to specific transaction postings to the general ledger. Unauthorized, undocumented adjustments can be made to the utility billing system customer master file, changing the customer receivable balance without appearing on the customer account history. These two features were not assigned any security and can be accessed by all district staff.

Sentencing. The accounting clerk pleaded guilty to first degree theft on March 27, 1998. Exceptional sentencing guidelines were used. She was sentenced on June 5, 1998, and served 33 months (2.75 years) confinement in the custody of the Washington State Department of Corrections at Purdy.

City of Battle Ground - $49,895

Schemes. Three individuals were involved in this case: the Clerk/Treasurer, her daughter (a city cleaning contractor), and the utility clerk (who was living with her son, a convicted criminal). Nepotism.

($37,664) Theft of cash receipts (currency) by the utility clerk in an Eden utility accounts receivable system environment. All cash receipt transactions were first processed on a Quadrant cash register system which produces data for the city's financial statements. At the end of the business day, these transactions were interfaced with the Eden utility accounts receivable system (stand alone computer) which marked all customer's accounts "paid". The utility clerk then reversed the initial transactions from Quadrant and re-entered only customer's accounts paid by check (lesser amount). The Quadrant system total report reflecting this reduced amount of revenue was then attached to and agreed with the bank validated deposit slip. The currency was simply stolen. To eliminate the audit trail, computer records for the prior transaction postings were deleted from the system, and hard-copy reports were destroyed. These changes were posted at unusual times of the day, and bank deposits were delayed for up to 47 days until computer records could be altered. There was little or no currency in the city's bank deposits. This scheme actually began by writing-off customer account balances without authorization or approval after funds were stolen. The utility clerk was also overpaid in payroll and caused the city to pay for a personal purchase by falsifying a vendor invoice.

($8,981) The Clerk/Treasurer charged personal purchases on the city's credit card. In most cases, only the summary charge slip was on file. However, some cash register tapes were altered to delete the detail of items purchased. Personal purchases included a computer and related software, computer games, and tools. The city's check register was falsified to conceal shortages of funds in the municipal court. Two checks issued were omitted from the check register, and utility deposit amounts were reduced to offset these transactions. Another check was prepared to conceal one of these transactions, but it never cleared the bank. The Clerk/Treasurer was also overpaid in payroll.

($3,250) The Clerk/Treasurer overpaid her daughter, the cleaning contractor, for services rendered. Payments were always made in advance of duties being performed (lending of credit issue). Payments for the four extra monthly payments were made by using manual warrants, and there were no supporting documents for these unauthorized transactions. These disbursements were not approved by the auditing officer or the governing body.

Detection. The city received many utility customer complaints over several months regarding the timeliness of account postings and delays in depositing checks. Other city employees noticed that the amount of "closing" cash from one day did not equal the amount of "opening" cash on the next day, and there was not enough currency in the cash drawer to make change for customers. The currency from four delayed deposits was then found to be missing. The city confronted the utility clerk who then confessed to taking cash from the delayed bank deposits to pay bills (with the intention of paying it back -- borrowing). Our audit detected additional utility losses, mid-month payroll draws which were not properly deducted from end-of-month payroll, overpayments on the cleaning contract, and personal purchases made by both the utility clerk

and the Clerk/Treasurer. The utility clerk and Clerk/Treasurer were terminated during the audit. In addition, the cleaning contract was canceled.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Segregation of duties problem. The utility clerk performed all tasks, including billing, collecting, depositing, posting and adjusting accounts, preparing accounting reports from computer systems, and handling customer feedback. City employees were aware that creditors frequently contacted the utility clerk at work about paying her debts. The Clerk/Treasurer both audited and approved city expenditures for accounts payable and payroll, was the primary signatory on city warrants, reconciled the checking account, and posted the general ledger. There was no oversight or monitoring of the work performed by the utility clerk or the Clerk/Treasurer.

(2) Adjustments to customer accounts were not authorized or supported. Some adjustments were labeled as "computer errors". Customer feedback also went directly to the utility clerk

(3) No one reconciled the Quadrant cash register system with the Eden utility accounts receivable system, and no one noticed that computer accounting records had been destroyed (after records had been altered).

(4) There were multiple cashiers in city hall, and all cash collections were commingled into one cash drawer.

(5) Computer passwords were not properly used (data integrity issue). After the first cashier reported for duty and signed-on the computer with their password, all other cashiers simply recorded transactions on the system throughout the day. As a result, all transactions are recorded in the system as if they were processed by only the one cashier who signed-on. Cashiers weren't identified in the data base with the transactions they processed.

(6) Deposits were not made intact daily. Delays routinely exceeded 30 days. The city's checking account was not reconciled timely (3 month delay), and the account was not reconciled by an independent party. The check register was maintained in pencil.

(7) The Clerk/Treasurer approved disbursement vouchers and signed city warrants without properly auditing the source documents for each transaction. Altered and improperly supported transactions were not noticed or investigated.

(8) The Clerk/Treasurer approved and signed payroll draws that were in excess of the amount due and the number of transactions allowed by city policy and state law. Overpayments were made to the utility clerk and the Clerk/Treasurer because the proper amount of mid-month payroll draws was not deducted from end-of-month payroll warrants.

Detection Steps.

(1) Review internal controls to ensure proper separation of duties. In accounts receivable operations, the duties of billing and posting/adjusting functions should be separated from the cashiering and depositing functions. In cash disbursement operations, the auditing officer should not be permitted to approve purchases they initiate. The work of these employees must be reviewed and monitored. Determine whether anyone involved in purchasing is **acting out of character** by performing tasks that they would not normally be expected to perform.

(2) Properly perform unannounced cash counts on all authorized funds and cash receipts. Analyze the composition of selected bank deposits and scan stub batches for irregularities. Determine whether deposits are made intact daily, and whether there is any cash in utility bank deposits.

(3) Use six audit steps from Fraud Manual accounts receivable section. Perform analytical procedures of revenue, cash in deposits, delinquent accounts/adjustments, universe of accounts, control and subsidiary account agreement, and agreement of total credits (from the Eden computer system) to bank deposits. Key steps in this case involved comparing accounts receivable credits to bank deposits and determining whether customer account adjustments were properly authorized and approved.

(4) Determine whether all checks are properly entered in check registers (sequence verification), and whether all voids are properly accounted for and controlled. If not available for review, make an inquiry of the bank to determine whether voided checks subsequently clear the bank.

(5) Determine whether the amount of payroll actually paid for key officials is proper, particularly those involved in payroll preparation, authorization, or approval. Determine whether all mid-month draws are properly deducted from end-of-month payroll.

(6) Determine whether vouchers are properly supported by the correct receipt for the type of transaction involved. Be alert for document alterations and falsifications, such as by using "white out" to conceal transaction data and by "cut-and-paste" actions to eliminate the detail for items purchased. Credit card purchase transactions and hand-written entries on receipts which list the nomenclature of items purchased are especially high risk.

Sentencing:

The utility clerk was sentenced to 21 months in the state penitentiary for her part in this crime. She was also convicted of felony counts in two other unrelated fraud cases involving stealing funds from her grandmother and illegally receiving welfare from the State of Washington.

The clerk/treasurer was sentenced to 3 months on a work release program.

City of Poulsbo (Municipal Court) - - $290,227.35 Loss (06/25/96 – 12/12/02)

The Court Administrator (age 44) misappropriated at least $290,227.35 in public funds from the City of Poulsbo Municipal Court for 6.5 years. The two revenue streams involved were manual

cash receipts and collection agency receipts. The first loss occurred 15 days after the employee started working at the Court. District Court Information System (DISCIS) accounting records were falsified in an attempt to conceal these losses by processing non-cash credit transactions, such as by adjudication of the fine or by indicating the individual had performed community service work. The loss is covered by the City's insurance bonding policy. No federal funds were involved in this case. The schedule below summarizes these losses:

Description	**Amount**
Citizen payments recorded on manual cash receipt forms were not entered into the DISCIS accounting system. There were 49 irregular transactions between 03/03/98 and 12/12/02.	$ 5,127.00
Collection agency payments were never recorded at the Court. There were 254 collection agency checks made payable to the Court that were deposited in the Court Administrator's personal bank account between 06/25/96 and 12/11/02.	285,100.45
Total Losses	$290,237.45

Detection Method. A temporary employee remembered that one citizen paid a $310 fine at Night Court using three $100 bills. Manual cash receipt forms are used in the Night Court operation. There were no such denominations of currency in the Court's cash receipts the following day. This irregularity was reported to City officials who investigated the transaction and discovered the loss.

City Investigation and SAO Audit. The City immediately performed an investigation and determined that $5,127.00 had been misappropriated from manual cash receipts. SAO reviewed the City's investigation and agreed with its findings and conclusions. However, in answering the question "What other revenue streams are at risk?", we discovered that collection agency checks to the Court were not properly recorded in the DISCIS accounting system. We obtained a copy of one of these checks from the collection agency and found an endorsement proving that it had been deposited into the Court Administrator's personal bank account. We then issued bank subpoenas for her personal accounts and worked directly with the collection agency and the Kitsap County Sheriff's Office to obtain copies of the misappropriated checks documenting a loss of $285,100.45.

Internal Control Weaknesses. The former Court Administrator performed incompatible duties when she substituted for other employees who normally worked in the cash receipting function. The City did not review her work to ensure that all transactions were properly entered into the DISCIS accounting system and all funds deposited in the bank. This enabled the employee to process irregular transactions without detection for approximately 6.5 years.

- Transaction information from manual cash receipt forms was not entered sequentially into the DISCIS accounting system. Deposits were not made intact daily, with delays ranging from two to 32 days. Generic cash receipt forms were used.

- No one monitored the various non-cash credit reports to ensure that all transactions were authorized, approved and properly supported. These include reports for restitution out-of-balance, restitution adjustments, accounts receivable adjustments, accounts payable adjustments, adjustment receipts, overpayments, and deleted accounts.

- No one monitored the accounts receivable system to ensure that all funds were properly collected and deposited in the bank. In addition, the Court's accounts receivables were not recorded in the City's accounting system or monitored by the Finance Department.

Recommendations. Referral to Prosecutor, restitution of loss amount ($290,227.45) and audit costs ($17,034.71), and improved internal controls to safeguard funds at the Municipal Court.

Sentencing: The employee pleaded guilty to 10 counts of first degree theft in Kitsap County Superior Court on March 12, 2003, and was sentenced to 57 months in jail, the top of the standard sentencing range for this embezzlement, on April 18, 2003.

Edmonds School District - $143,150 Loss (1996-2002)

The Accounts Receivable Bookkeeper (age 49) at the Business and Operations Department's central office misappropriated at least $143,150 for at least 7 years. While the former employee began taking currency from transmittals from decentralized locations and other departments in the District, she reportedly made these cash receipting locations whole from other sources and subsequently confined her activities to taking funds from the District's accounts receivable system for billings to other Districts and from other miscellaneous revenue transactions. District accounting records were falsified to conceal these losses from managers. Because of these complex manipulations in the District's daily bank deposits during this period of time, it would not be practical or cost effective to determine the full extent of this loss. The loss is covered by the District's insurance bonding policy. No federal funds were involved in this case.

Detection Method. By letter of November 26, 2002, the former bookkeeper's attorney informed the District of her resignation and admission to misappropriating public funds. This was in response to the District's questioning of the employee's cash handling practices on a number of occasions. The employee was unable to respond to the most recent irregularities noted by the District and realized that she would not be able to continue her past practices.

District's Investigation and SAO Audit. Based on advice and guidance given by Team SI, the District immediately performed an investigation and determined that $143,149.79 had been misappropriated from cash receipts. The sources of these revenues included: (1) accounts receivable balances written-off when customers proved the outstanding amount due had previously been paid ($86,675.60); and, (2) unrecorded revenue from decentralized locations and miscellaneous sources that were deposited to the credit of others in the accounting system ($57,046.69), less checks on-hand from these transactions that had not yet been deposited in the bank ($572.50). We reviewed the District's investigation and agreed with its findings and

conclusions. The District and Team SI also interviewed the former bookkeeper and subpoenaed her personal credit union account. The credit union was unable to provide the detail of any bank deposits because they did not microfilm deposit records for individual accounts.

Internal Control Weaknesses. Internal controls over cash receipts at the central office were inadequate.

The employee had incompatible duties and was thus able to circumvent District procedures and manipulate the content of the District's daily bank deposits without detection for many years. The employee was responsible for practically all aspects of the accounts receivable system including processing transactions for billings, posting customer accounts for all payments, processing all revenue from customer cash receipt transactions, and receiving customer and department feedback about questions on accounts. The employee was unable to write-off the balance of any accounts receivable account.

The employee performed cashiering duties and processed transactions and funds from accounts receivables, decentralized locations at schools and in other departments, and miscellaneous revenue from other sources. She was solely responsible for opening and counting funds transmitted to the central office from all cash receipting locations throughout the District. Employees did not exchange accountability for money when funds were transferred from these cash receipting locations to the central office cashier, such as by signing documents fixing responsibility for funds. She also processed funds received through the mail and created transmittal forms to account for the money. However, no other cash receipting records were created to establish accountability for these funds that arrived through the mail.

Deposits were not made intact daily. While an independent party verified the total amount of the bank deposit, this individual did not properly monitor daily activity by verifying that the check and cash composition of the bank deposit agreed with the mode of payment for all transactions recorded in the District's cash receipting records. In addition, the Business and Operations Department did not prepare a summary transmittal document identifying all sources and funds collected by decentralized locations, other departments, and the central office.

The District's transmittal forms were not prenumbered or otherwise monitored using some other type of accountability system designed to ensure that transmittals and funds from all cash receipting locations were properly accounted for and controlled. The former Accounts Receivable Bookkeeper manually assigned control numbers for the transmittal forms after they were received at the central office.

The District relied upon the decentralized locations and other departments to verify that all funds transmitted to the central office were properly deposited and recorded in the District's accounting system. However, all cash receipting locations did not systematically perform this function. The former Accounts Receivable Bookkeeper altered many transmittal forms and entered inaccurate information in the District's accounting system after a turnaround copy of the original document had been returned to the various decentralized cash receipting locations. However, the staff did not identify these irregular transactions.

The Transportation Department maintained its own accounts receivable system. This information was not recorded in the District's accounting system or reported on its financial statements.

Recommendations. Referral to Prosecutor, restitution of loss amount and audit costs, and improved internal controls.

CASH REGISTER SCHEMES

Cashiers perpetrate cash register schemes by voiding valid transactions to reduce total cash accountability, making bank deposits in these reduced amounts, and stealing the difference. Thus, "voids" are a high risk transaction.

The danger in auditing any cash receipting system is not knowing what type of cash register is in use, and what it can do to you and for you. For example, cash registers record voided transactions in two ways.

> Type 1. This cash register does not allow voids to be recorded during transaction processing. After cashiers record erroneous entries, the transactions must be aborted and totaled. A void document is prepared for this amount and approved by a supervisor. The cashier completes this transaction by entering the correct amount on the cash register. At the end of the day, this cash register includes all inappropriate transactions in the total accountability. Thus, a reconciliation is required to establish total cash accountability for the bank deposit. The computation is gross sales, less voids, equals total cash accountability and bank deposit.
>
> Type 2. This cash register allows voids to be recorded during transaction processing. At the end of the day, it reports only the net cash accountability (i.e.; no reconciliation is required as above). Since void transactions are recorded only on the cash register detail tape by a minus sign next to the applicable entry, a review of the detail tape is mandatory. This is a high risk environment.

Basic Cash Register Operations.

Two primary control key positions on all cash registers are:

> "X". This is a sub-total key used to determine cash receipts status periodically and at shift changes.
>
> "Z". This key closes the business for the day, and presents totals for the daily activity report and bank deposit.

Two primary manufacturer controls (i.e.; numerical counters) maintained internally in all cash registers are:

> "Z" tape. Each time the "Z" key position is activated, a numerical counter adds one to the previous balance recorded in the cash register. This number is printed on a "Z" tape,

along with all pertinent control totals from the machine. "Z" tapes are a prenumbered accountable form.

Cumulative sales total. Each time the "Z" key position is activated, the total of all sales from the business day is added to another numerical counter containing the life-to-date balance recorded on the machine. This amount is included in the control totals printed on the "Z" tape.

Red Flags:

Inappropriate employee segregation of duties.

Cashiers, rather than supervisors, have access to the control keys which are inserted in the cash register at all times.

Cash registers are operated in an open cash drawer mode.

Multiple cashiers operate from a single cash drawer.

Appropriate forms are not used for the support and supervisory approval of all voided transactions.

All copies of voided cash receipt forms (manual systems) or supporting documents for voided transactions (cash register systems) are not retained on file.

Cash register "Z" tapes are not in sequential order (i.e.; some are missing).

Fraud Detection:

Review the segregation of duties of key employees.

Observe cash register operations during unannounced cash counts.

Review supporting documents for voided transactions for propriety (i.e.; legitimate and approved).

Review the numerical sequence of cash register "Z" tapes to ensure all prenumbered forms are properly accounted for and controlled.

CASE EXAMPLES

A port accountant stole $13,100 from marina fuel sales over a 7 year period of time. Marina employees issued receipts for all marina cash and charge sales as the transactions occurred. The accountant periodically visited the marina, recorded all fuel sales on the cash register, closed the day's business, and prepared the daily activity report. After returning to the main port office, the accountant reduced overall cash accountability by altering the daily activity report, issued a

receipt in the reduced amount from the centralized cash receipts journal, and made the bank deposit in an amount which agreed with the reduced total recorded cash receipts indicated for the day. Initially, the accountant wrote "void" on the cash register detail tape to reduce accountability for the funds stolen. When no one ever questioned this, the accountant ceased this practice (the chameleon effect). Thus, cash register accountability indicated one amount for cash receipts from fuel sales, while the cash receipts journal and bank deposit indicated another (reduced) amount. This fraud was missed by auditors who reviewed the centralized cash receipts (summary level documents) rather than the cash register detail tapes (original source documents). When the fraud was detected, the accountant had retired and moved to another state. A Type 1 cash register voiding system was used in this entity (i.e.; gross accountability).

A supervisor in a health district stole $16,400 from cash collections while acting in a relief cashier capacity. Full-time cashiers properly recorded all transactions on the cash register. During breaks and lunch, the relief cashier (supervisor) destroyed accountable documents, recorded "void" transactions on the cash register, and took an amount of cash equal to the transactions eliminated from accountability. Full-time cashiers did not notice the missing documents or the inappropriately voided transactions on the cash register detail tape. A Type 2 cash register voiding system was used in this entity (i.e.; net accountability).

TRAINING EXAMPLE

If you're reviewing the numerical sequence of "Z" tapes from a cash register and find that one is missing, use the procedures listed below to compute the total amount of accountability that is represented by the missing "Z" tape. In this example, assume that "Z" tape number 50 is missing from your test.

> Step Number 1. Subtract the cumulative sales total of "Z" tape number 49 from the cumulative sales total of "Z" tape number 51.
>
> Step Number 2. Subtract the daily sales activity shown on "Z" tape umber 51 from the result attained above in Step Number 1. These valid sales amounts are included in the cumulative sales shown on "Z" tape number 51 and must be eliminated from this computation.
>
> Step Number 3. The result of the computation shown above in Step Number 2 will be the amount of cash accountability that is actually reflected on the missing "Z" tape number 50.

Since the inner workings of the cash register can be easily demonstrated by a manufacturer's representative, this loss amount can be easily supported and used in court, if needed.

EXAMPLE

"Z" Tape Number 51: Cumulative sales total ($104,000); Daily sales activity ($4,000).

"Z" Tape Number 49: Cumulative sales total ($95,000); Daily sales activity ($6,000).

COMPUTATION

"Z" Tape Number 51 Cumulative Sales Total	$104,000
"Z" Tape Number 49 Cumulative Sales Total	(95,000)
Sub-Total	9,000
"Z" Tape Number 51 Daily Sales Activity	(4,000)
Daily Sales Activity On "Z" Tape Number 50 (Accountability)	$ 5,000

COMPUTER CASH RECEIPT SCHEMES

Since perpetrators commit computer frauds and manual frauds exactly the same way, most computer fraud is really computer assisted fraud. The computer simply allows employees to process fraudulent transactions faster and for larger amounts. These schemes will also be observed and detected in other areas through normal substantive audit tests of cash receipt transactions.

Personal computers. Many small entities use personal computers for accounting and reporting purposes. There are no internal controls in this environment because anyone can change data on the computer disks at any time without leaving a record of who made the change, when, or why. Therefore, beware!

Computer back-up systems. When computer cash receipting systems are used, entities retain manual cash receipting procedures and forms as back-up for use when: (a) there are periods of high transaction volumes; (b) the computer is down for scheduled or unscheduled maintenance; (c) there is a power outage; and, (d) transaction accountability has not yet been entered on the computer (input cannot be accepted).

- Computer processing. During normal cash receipt processing, employees record cash receipt transactions on the computer system which then issues official prenumbered cash receipt forms to customers. These receipts indicate mode of payment, and daily activity reports are prepared indicating the check and cash composition of all transactions. The daily bank deposit is prepared solely from transactions recorded on the computer system.

- Manual processing. When the computer is down, cashiers initially record cash receipt transactions by issuing official prenumbered manual cash receipt forms to customers. These transactions are subsequently entered on the computer system and cross-referenced (both ways) to ensure that all transactions are properly accounted for and controlled. Supervisors must compare manual records to computer records to ensure that all transactions are properly recorded, because all internal controls are designed around the computer cash receipts system which produces the daily activity reports.

Computer passwords. Internal control procedures for access to safes and vaults and their combinations also apply to computer passwords. Computer passwords must be issued by systems managers, and changed periodically thereafter by operators. Some systems have automatic lock-outs if operators fail to change passwords within a prescribed frequency. Passwords must not be written down in the office or given out to unauthorized personnel, and must be deleted when employees terminate employment. Computer operators and users must be identified with the transactions they process in the data base.

Non-cash credit transactions. The most common form of non-cash credit transactions involve community service time worked or jail time served in municipal and district court systems. These transactions must be: (a) processed by individuals who do not perform the cashier function (full-time or relief); (b) reviewed and approved by a supervisor; and, (c) recorded on the

citation document. These transactions must be listed on daily exception reports, and be monitored and certified by supervisors. Supporting documents must be retained and filed by individuals who have no responsibility for processing this type of transaction.

Cashiers perpetrate frauds in both manual and computer accounting systems by processing fictitious non-cash credit transactions to eliminate accountability for funds received from customers. No attempt is made to cover-up these transactions, because cash receipt documents are usually issued to customers for the amount of funds actually received. However, there are no supporting documents for these unauthorized non-cash credit transactions. Funds equal to the amount of the fictitious non-cash credit transactions are then stolen. A "void" transaction in any manual cash receipting function accomplishes the same purpose.

Red Flags:

- Inappropriate employee segregation of duties. Individuals entering accountability for transactions on the computer should never have cashier responsibilities, even in a relief capacity.

- Entity uses a personal computer for accounting and reporting purposes.

- No one compares manual cash receipt forms issued to subsequent computer cash receipt forms to verify that all transactions were properly input.

- Inappropriate access to the computer facility or to operator passwords (i.e.; unrestricted access or too many people).

- Computer system whose operator passwords do not identify the user with transactions they process in the data base.

- Computer system which does not prepare a report listing total subsidiary ledger card postings for comparison to daily bank deposits.

- Computer system which does not prepare a daily activity report listing the check and cash composition of cash receipt transactions for the daily bank deposit.

- Computer system which does not prepare reports identifying any unusual, exception, or special authorization transactions (such as non-cash credits) for review and approval by supervisors during routine processing at the end of the business day.

Fraud Detection:

- Review the segregation of duties of key employees.

- Determine whether personal computers are used for accounting and reporting purposes.

- Compare manual cash receipt forms to subsequent computer cash receipt forms to ensure that all transactions are properly recorded.

- Review the computer operator password access system for propriety.

- Review critical computer exception transactions (particularly non-cash credits, and cancellations or deletions of accounts and account balances) to ensure that all items are valid, properly supported, and approved by a supervisor.

CASE EXAMPLES

Use of personal computer for accounting and reporting purposes. A supervisor of cashiers at a university stole $470 from tuition fees at a decentralized department location. Cash receipt transactions for each business day were identified on the department's personal computer system by cash transmittal number. Cashiers initially receipted these transactions, recorded them on a computer disk, prepared the daily activity report, and transferred all funds and records to the supervisor. This individual then altered these records by accessing the computer disk, changing (lowering) the cash transmittal number of each transaction where the mode of payment was by cash (i.e.; currency) to delete these transactions from the days business totals, preparing revised daily activity reports, and making the bank deposit in this lesser amount. All check transactions were deposited, but all cash transactions were stolen. All students were appropriately registered for classes.

Comparing manual and computer cash receipt forms. Relief cashiers in two municipal courts stole $4,200 and $700, respectively, from traffic citation payments. While manual cash receipt forms were issued to customers, these payments were not subsequently recorded on the computer cash receipting system. Managers failed to compare these two records to ensure that all transactions were entered on the computer system and that all funds were properly accounted for and controlled.

Abuse of computer passwords. A computer security director responsible for assuring the company's password system worked properly decided to get revenge on his employer, a securities trading firm. Initially, he took up a tax protest cause, arguing with his superiors because he wanted to be exempt from withholding taxes. They said no. He kept trying. One day he was preparing papers to sue the firm when another employee noticed him using the company computer to do this. He was fired and told to turn in his keys. Sales for this nationally licensed life insurance agency and registered securities broker were made through 450 independent agents who received $2 million in commissions each month. After an employee prepared a preliminary monthly report, he began checking certain detail records. When accessing the computer the second time, the records couldn't be found. Further research proved that over 168,000 computer records had disappeared, making the monthly payroll impossible. When a history log was prepared listing access, accounts used, passwords of people using them, and time of use, the employee noticed an unrecognizable password which eventually led the company to the perpetrator. Even though his computer password access had been changed, this employee entered the building 3 days after he was fired using a duplicate office key. He then used a secret trap door to access the computer, assigned himself a password, and built a program (worm) to destroy the records. It took the entire staff 3 days to reconstruct the damage done by this revengeful employee.

Fictitious non-cash credit transactions.

Court computer cash receipting system (traffic fines and fees). A cashier and a supervisor of cashiers stole $13,000 and $37,800, respectively, by processing fictitious non-cash credits (i.e.; community service time worked or jail time served) in a district court after customers paid cash for traffic citation fines and fees. All transactions were initially recorded on manual cash receipt forms issued to customers. However, these documents were not cross-referenced to computer cash receipt forms when these transactions were formally recorded in the computer accounting system. The supervisor used her own computer password for some of these transactions, and the computer passwords of multiple cashiers in the office for the remainder of these transactions (had inappropriate access to these passwords). The completed citations for these transactions were on file within the court (i.e.; all marked "paid"). The court did not verify that all manual cash receipt transactions were subsequently recorded on computer records, and did not produce exception reports for supervisory review and approval of all non-cash credits entered into the system. There was no review and oversight function to detect non-cash credits which were processed using transaction types where these credits were not authorized in the system (inadequate computer transaction edits).

County treasurer computer cash receipting system (property taxes). A property tax clerk in a county treasurer's office stole $185,400 through the property tax cash receipting process. The fraud was a three step process. First, cash was removed from the daily bank deposit by using a check for cash substitution scheme. Since locking bank bags were not used, this clerk revised the composition of the daily bank deposit while en route from the county to the bank. Checks which taxpayers sent through the mail for real property tax payments were the source of the unrecorded checks used in this scheme. The tax clerk retained the customers copy of the tax statement as a record of all accounts which had been manipulated. Second, the property tax clerk subsequently processed cash receipt documents indicating these manipulated accounts were paid from funds held in a tax suspense account (even though funds had never been placed in the suspense account for this purpose). Thus, customer feedback did not occur because these manipulated accounts never became delinquent. Finally, the account balances of unrelated personal property taxpayers whose funds were legitimately held in suspense (advance tax payments) were written-off by using a computer software program designed for this purpose. This final action compensated for the fictitious payment transactions indicated in step two above, and avoided detection of the imbalance in the suspense account. The county treasurer's computer system did not produce exception reports for supervisory review and approval of all tax cancellation transactions entered into the system (no review and oversight function for this high risk transaction type).

College cash register system. College cashiers stole $3,700 from tuition fees and other miscellaneous revenue sources by accomplishing the following during transaction processing: (a) all transactions were initially recorded on the cash register; (b) certain cash register validated documents were destroyed; (c) fictitious "void" transactions were entered in a manual log to eliminate accountability for funds (no approval or support was required); (d) bank deposits were made in an amount equal to the reduced accountability for the day; and, (e) an amount equal to the amount of the fictitious "void" transactions

was then stolen. No one was able to fix responsibility for these losses because the college regularly used multiple cashiers on a single change fund and cash register. All cashiers passed lie detector tests. In response to the personnel application question: "What do you like best about cashiering?", one of the two primary suspects in this case responded: "Manipulating cash." There were also 20 internal control weaknesses cited in the audit report covering only cash handling procedures.

CASHIERS WHO PLACE PERSONAL CHECKS IN THE TILL DRAWER

This is the most common scheme used to borrow funds from an entity. When a cashier doesn't have enough money to make it from one payday to the next, they often abuse the change fund (and possibly cash receipts too) by placing a personal check in the till drawer. When payday arrives, they redeem the check by replacing it with cash. If the initial check isn't large enough, the cashier may even replace it with another one for an even bigger amount. If the amount of the free loan gets too large, the cashier may even skip a payday without redeeming the check. In these instances, the check may be replaced with another one with an updated (current) date. If ever questioned about this check, the individual explains it away by stating that they just cashed a check for themselves. If management requires this check to be deposited, it may be returned for non-sufficient funds (NSF). Follow-up work must be accomplished to determine whether this actually occurred, and whether payment was subsequently received by the entity.

Red Flags:

- One or more personal checks from the fund custodian, perhaps stale-dated, are found in the till drawer.
- Deposit timing lags (delays).

Fraud Detection:

- Be observant of all activity during unannounced cash counts.
- Analyze prior bank deposits for presence of a consistent pattern of checks from fund custodians and cashiers.
- NSF checks are not subsequently collected by the entity

CASE EXAMPLE

A school district fiscal clerk at a central treasurer function borrowed $2,400 by placing 23 personal checks in deposits which had been made from various student activities at decentralized locations. This individual placed a personal check in each deposit as the method used to keep track of the amount of funds that had been borrowed. These transactions had been inappropriately delayed for up to 5 months. Auditors detected this condition during an

unannounced cash count. On that date, the fund custodian had only a few hundred dollars in their bank account (telephone confirmation from the bank which was authorized by the employee). When all 23 personal checks were deposited in the district's account, several of the larger checks were returned as NSF. All checks subsequently cleared the bank upon re-deposit (after payday). The fiscal clerk's employment with the district was terminated.

CASHIERS WHO COLLECT THE MONEY AND STEAL IT

This is probably the method of choice preferred by smart crooks in any entity. Employees simply collect funds from customers and steal the money. They do not record any official accountability for these funds, either by preparing a cash receipt form or by recording the transaction on a cash register or computer cash receipting system.

Red Flags:

- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.

- Revenue projection using alternative records reveals a significant decline in a local revenue source.

- Observation of procedures used at a cash receipting function reveals a cash skimming operation.

Fraud Detection:

- Perform analytical review procedures on all local revenue sources.

- Use alternative records to verify the reasonableness of all local revenue sources.

- Use marked money or covert surveillance procedures (i.e.; film or video camera) to confirm conditions when fraud is suspected. This is an extraordinary audit test.

CASE EXAMPLES

Four cashiers and equipment operators at a county landfill site, working in collusion with each other, stole $165,200 by taking cash receipts from landfill user fees. These funds were stolen before these cash receipt transactions were recorded (i.e.; no records). These individuals circumvented the county's system of internal control over landfill cash receipts. Covert surveillance procedures were used (i.e.; video tape cameras) to prove that cash receipts were being stolen. Computer cash registers linked to the landfill weight scales provided the data base necessary for analytical review procedures of the historical cash receipting activity of each landfill cashier (i.e.; by cashier, shift, day of the week, and amount). These records proved that the individuals involved in this scheme collected significantly less revenue than honest cashiers who worked on the same shift and on the same day of the week. However, these computer

records were available for only a nine month period (scope limitation). The actual loss is much higher than indicated.

An irrigation district secretary and a county building department cashier established checking accounts in the name of the entity and stole $54,300 and $3,100, respectively, by depositing checks from customer payments into these accounts which were under their control. These bank accounts were used to convert public funds to private use, because all disbursements from them were made to themselves.

A county building department cashier accepted a $1,600 check from a customer and entered her own name on the payee line in order to cash it for personal gain (forgery). The customer complained to the county about the irregular check endorsement on his canceled check after it had been redeemed by the bank.

A college employee stole $5,400 from football athletic gate receipts, and a school district advisor stole $1,100 from student dance receipts. No documents were maintained to establish the amount of revenue generated from these events.

A school district business manager stole $10,600 from lunchroom receipts. Decentralized activity revenue records were used to establish the amount of funds missing at the central treasurer function.

Toll booth cashiers in the state ferry system stole $40,000 and $78,100, respectively, by collecting funds from customers without recording accountability on the cash register. An Internal Revenue Service type audit of their private bank accounts (i.e.; identify all illegitimate sources of income deposited) established the amount of these losses. An alternative record to verify the reasonableness of revenue is a physical count of the vehicles and passengers on the ferry.

Army National Guard employees stole $2,000 and $2,300, respectively, from armory room rental fees. Armory reservation records (alternative records) were used to determine which organizations used the facility and which funds could not be properly accounted for in the unit's bank account. Confirmations from the organizations where no payments were noted obtained the documents (i.e.; cash receipts and cancelled checks) needed to prove the amount of the loss. Park cashiers in a county and state facility stole $5,700 and $2,300, respectively, from camper user fees. Differences between cash register entries and daily logs of occupied camp sites (alternative records) established the amount of these losses.

A sheriff's department employee stole $3,200 from the jail work release laundry facility and a private non-profit organization associated with the sheriff's department. The amount of funds collected from washing machines was entered in unofficial department records, but never deposited with the central treasurer function. An analysis of average revenue compared to inmate population before the current employee assumed this duty, and while the current employee performed this duty, established the amount of this loss.

CASHIERS WHO ESTABLISH THEIR OWN ACCOUNTABILITY

A cashier who has the ability to establish their own accountability for funds is the most dangerous person in the world. This situation occurs when revenue from any source is turned-in to the central treasurer function by someone from a decentralized cash receipting location without formally counting the money when the exchange occurs. The funds are merely dropped-off without being counted or officially receipted at the time the transaction occurs. The decentralized location relies upon the central cashier to count these funds at a later time. Revenue is exactly what the central cashier says it is, even though it's not necessarily the same as the amount of funds the decentralized location activity actually turned-in (usually less).

Red Flags:

- Inappropriate employee segregation of duties.
- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.
- Revenue projection using alternative records reveals a significant decline in a local revenue source.
- Observation of procedures used at the central treasurer function reveals that funds are not counted when turn-ins are made from decentralized cash receipting locations.
- Timing lags (delays) exist between cash transmittals from decentralized cash receipting locations and receipt of funds at the central treasurer function.

Fraud Detection:

- Be observant of all activity during unannounced cash counts.
- Perform an analytical review of all local revenue sources.
- Use alternative records to verify the reasonableness of all local revenue sources.
- Agree (compare) the amount of cash receipts shown at the central treasurer function with the amount of cash receipts recorded at decentralized cash receipting locations for the same transaction or event.

CASE EXAMPLE

A city clerk stole $4,300 from landfill user fees which were initially receipted by a landfill attendant, but which were subsequently recorded in the city's records at a lesser amount. The money was not counted or receipted by the city clerk when the landfill attendant turned-in both cash receipt forms and funds at the end of each business day. When the clerk issued the city receipt to establish accountability for the funds, these receipts were issued for amounts which

were routinely $20 less than the amount which was actually turned-in. The loss was proved by comparing total landfill cash receipts (original source documents) to the city's total cash receipts (summary level documents). All landfill cash receipt forms from prior accounting years were destroyed (one year loss amount only) after each audit because the city clerk knew these records would prove the amount of the loss (if detected). The fraud perpetrator worked at the city for 15 years (tip of the iceberg).

WSU Animal Sciences Department - $43,355

Scheme. Largest decentralized location cash receipts fraud case. A fiscal technician (centralized cashier) took funds from revenue produced at decentralized reporting locations within the department by taking currency from recorded cash receipt transactions, using a check for cash substitution scheme, and depositing WSU checks from both recorded and unrecorded transactions into her personal credit union account for over six years. Funds were also skimmed from unrecorded cash receipt transactions as evidenced by unexplained cash deposits of $22,212 in the cashier's personal credit union account. Higher losses are probably, but cannot be proved. Cash receipt records were falsified and destroyed to conceal these losses. Deposit records retained at the department were different from those officially filed with the WSU Controller's Office.

Detection. A student in the Cooperative Horse Organization Serving Students (C-HOSS) Program questioned two personal checks issued to WSU which had been altered to show the cashier's name on the payee line and deposited into the cashier's personal credit union account. The cashier confessed to taking $2,731 from the C-HOSS Program when confronted with these checks by department managers. She was then allowed to exhaust her leave balance and resign. The Department Chair made a personal loan to the cashier for restitution purposes.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Segregation of duties problem. Cashier received all revenue from multiple decentralized locations within the department, issued cash receipts, and made deposits with the WSU Controller's Office. Her work was not properly supervised or monitored.
(2) Cash receipt documents were not monitored at the department or the WSU Controller's Office. Thus, falsified documents were not noticed at the department, and critical document verification steps were not taken at the WSU Controller's Office. While cash receipt forms were filed numerically, no one verified the accuracy of forms, amounts, or budget coding reported on Cash Deposit Reports.

(3) Deposits with the WSU Controller's Office were not made promptly or intact. In addition, department copies of Cash Deposit Reports were not always validated to prove that the cash receipts were actually deposits (i.e.; same as bank-validated deposit slips).

(4) Controls over cash collections at decentralized reporting locations within the department were non-existent. Funds were not always receipted at the point of origin. When funds were turned-in or transmitted to the cashier, activity reports were not prepared which summarized key transaction data elements for all cash receipt transactions, such as sequential use of prenumbered official receipt forms, housing occupancy reports, gross profits testing from sales of inventory

items, and "Z" (total accountability) tapes from cash registers. Thus, no one was able to monitor the accountability for funds within or from these locations. In addition, the cashier occupied the most dangerous position in the world because she was able to establish her own accountability for funds.

Detection Steps.

(1) Review cash receipting controls and fund transmittal systems at decentralized locations. Expand audit testing when significant weaknesses are noted. Ensure proper separation of duties for key employees. Perform analytical procedures for revenue and cash in deposits.

(2) Properly perform unannounced cash counts. Analyze the composition of selected bank deposits and verify to bank-validated deposit slips. Find a way to intercept decentralized location turn-ins for analysis before they are commingled with a central treasurer's bank deposit or deposited in the bank.

Other. Expand recommendations to include other areas when needed. In this case, we also recommended WSU review cash receipting procedures in other departments to ensure that internal controls over cash receipts have been properly established and are periodically monitored.

CASHIERS WHO ALTER CASH RECEIPTS AFTER ISSUE

This scheme is perpetrated by a cashier who collects money for the many and varied services provided by any entity, and documents these transactions by using multiple-part cash receipt forms. The typical receipt book has three receipts to a page, and three copies which are distributed as follows: (a) white is the original copy for the customer; (b) yellow is the accounting copy; and, (c) blue or pink is the copy that remains in the receipt book as a permanent record.

There are two ways to commit this fraud. In both cases, the cashier removes the original copy of the receipt from the book at some point during the transaction.

- In the first method, the cashier removes the original copy of the receipt form from the receipt book before completing and issuing it to the customer. All data entries on this original cash receipt form copy (stand alone document) are then completed by the cashier.

- In the second method, the cashier completes all data entries on the cash receipt form (intact within the receipt book), except for the amount of the transaction. The cashier then removes the original copy of the receipt form from the receipt book before completing and issuing it to the customer. The amount entry on this cash receipt form (stand alone document) is then completed by the cashier.

By processing transactions in this manner, the customer receives a receipt for the amount actually paid for the service received. After the customer departs, the cashier then completes the

remainder of the receipt in an amount which is less than what the customer actually paid. Once this has been done, the total of all cash receipts issued each day will agree with the bank deposit subsequently made.

- The most common method used by cashiers is to complete the remainder of the cash receipt form with a ball point pen (ink). The attribute about these cash receipt forms which indicates that a fraud has been perpetrated is the fact that the accounting copy of the document (yellow copy) has been prepared in ink when it's supposed to have been prepared in carbon. All transactions of this type are not necessarily fraud, because sometimes cashiers forget to put the carbon paper back in the book, or put the carbon paper in backwards, when page changes are made. Corrections of subsequent (valid) transactions are then made in ink. A few transactions of this type should not be a matter of great concern; however, routine transactions of this nature are a cause for alarm. Confirmations with customers, if practical, are the primary method used to complete a subsequent investigation and prove the amount of any loss.

- The next most common method used by cashiers is to again complete the remainder of the cash receipt form. However, this time the cashier uses a blank form from the back of the book, or from some other voided cash receipt form, to replace the original copy in the book. This document is placed on top of the other receipt copies in the book to simply align the blocks on the form so that the reduced amount shown on the accounting copy of the document will be in the correct position, and will also be in carbon. If you ever find a receipt form in a cashier's work area which has been written over many times, confiscate the document and the cash receipt book immediately because these documents are needed (evidence) to prove that the fraud occurred and to establish the amount of the loss.

Red Flags:

- A large number of the accounting copies of cash receipt forms are written in ink rather than in carbon.

- A single cash receipt form is found in the cashier's work area that has been written over many times.

- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.

- Revenue projection using alternative records reveals a significant decline in a local revenue source.

Fraud Detection:

- Be observant of all activity during unannounced cash counts.

- Perform an analytical review of all local revenue sources.

- Use alternative records to verify the reasonableness of all local revenue sources.

- Agree (compare) the amount of cash receipts shown at the central treasurer function with the amount of cash receipts due from customers, such as from some alternative record, for the same transaction or event. Use account or customer confirmations, when practical.

CASE EXAMPLES

An elected county treasurer borrowed $13,000 in property tax receipts by using a check for cash substitution scheme for part of the funds paid by customers, and repaying the amount initially stolen prior to the end of the tax period. During the tax year, each affected account was only marked paid for a half-year when the taxpayer actually paid full-year taxes. If any of these parcels of land had been sold during the year, these transactions would have come into question. This did not happen because all parcels of land were leased by absentee landlords (i.e.; out of town, and out of state). The treasurer made repayments by using the actual second half tax statement for these taxpayers (obtained at the county prior to mailing), and by processing cash payments through his treasurer's trust bank account (i.e.; account used for tax payments held in suspense) to avoid suspicion on the part of other office employees. Accounting records (cash receipts) were falsified in an attempt to conceal this loss. The amount of the office change fund fluctuated each day, the mode of payment was not indicated on cash receipt forms, and deposits were not made intact daily. When a sufficient amount of cash was available in the office, the treasurer altered transactions for individuals who paid full-year taxes at the beginning of the year by issuing an official receipt for the first half-year tax payment, deposited the check for the entire payment, and took the difference in cash. Receipts issued to taxpayers indicated that full-year taxes had been paid (falsification of records). In some cases, taxpayer checks were deposited in the bank up to 2 months prior to any receipt being issued by the treasurer (i.e.; he stole the entire amount for a period of time, and then adjusted the amount down to half that amount later). While the official receipts issued and on file in the treasurer's office were supposed to be in gray carbon color, all falsified transactions were written in ball point pen (ink). When all transactions written in ink were selected for confirmation with the taxpayers involved, the universe of all fraudulent transactions was included on that list. Not all transactions written in ink were fraudulent. Some transactions were valid errors or adjustments. This fraud occurred in prior years. But, since all accounts eventually were paid, the amount of the loss to the county in prior years only represented the amount of investment interest that was lost during the 6 month period of time the funds were not in the county's bank account.

A cashier at a central treasurer function in a statewide library system stole $482,800 in library fees over a multiple year period of time by manipulating cash receipt documents. While issuing cash receipts to decentralized libraries throughout the state for the correct amount that was transmitted, the accounting copies of these same receipts (prepared in ball point pen) were issued for lesser amounts. The bank deposits made agreed with the reduced amount of accountability for these funds. This fraud was detected during the budget process when an accountant noticed that library fee cash receipts recorded for the total state library system varied significantly (less) from that recorded for the total of all decentralized libraries.

CASHIERS WHO USE MULTIPLE RECEIPT BOOKS

This scheme is perpetrated by a cashier who collects money for the many and varied services provided by any entity, and documents these transactions by using multiple-part manual cash receipt forms. When Rediform cash receipt forms obtained from retail office supply stores are used by the entity, cashiers have the ability to purchase these receipt books for themselves in any numerical sequence desired. They then begin to receipt one transaction for the entity (check payments), and one transaction for themselves (cash payments). Then, they increase the level of illegal activity for themselves. If you ever find more than one cash receipt book in use for the same purpose, confiscate all books immediately because these documents are needed (evidence) to prove that the fraud occurred and to establish the amount of the loss. However, remember that multiple cash receipt books for varying purposes is a legitimate activity. Employees may also use receipts from the middle or back of these receipt books and not turn-in the money collected to accomplish the same purposes. As a result, we always recommend entities use official prenumbered receipts with the entity's name printed on them by the manufacturer for cash receipting purposes.

Red Flags:

- More than one cash receipt book for the same purpose is found in the cashier's work area.
- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.
- Revenue projection using alternative records reveals a significant decline in a local revenue source.

Fraud Detection:

- Be observant of all activity during unannounced cash counts.
- Perform an analytical review of all local revenue sources.
- Use alternative records to verify the reasonableness of all local revenue sources.
- When more than one cash receipt book for the same purpose is found in the cashier's work area, determine which receipts have been included in: (a) the bank deposit for a central treasurer function; or, (b) the cash transmittal to the central treasurer function for a decentralized location. All other receipts issued (usually an entire book) represent the fraud.

CASE EXAMPLES

The police chief and several successive municipal court clerks worked in collusion with each other to steal $45,300 from traffic citation payments. All cash receipt transactions were initially receipted using receipt books that had been discontinued from use in the court. Once these individuals decided how much money was to be deposited in the city's account, these transactions were then re-recorded on the court's official cash receipt forms (receipting transactions twice was hard work). Revenue in this court went consistently down from $25,000 to only $1,300 over a seven year period of time. When the city treasurer asked about the decline in revenue, the police chief told him not to worry because the funds were "tied up in trust". While only bail funds are placed in a trust account, this inappropriate explanation was accepted because the city treasurer did not understand the court's operation. Court employees were stealing 7 out of every 8 transactions when this scheme was finally detected by an auditor who discovered the extra cash receipt books in the court's vault. However, an analytical review of the court's declining revenue should have detected this fraud much earlier.

The Daystall Assistant/Market Master at Pike Place Market (Seattle) misappropriated daystall rent receipts totaling $173,875 over at least a three-year period. It was inefficient for anyone to determine the amount of additional losses in this case. The amount of recorded cash receipts did not equal the amount of funds deposited in the bank. The Market Master took attendance, collected daystall rent, issued receipts to vendors and reconciled daystall attendance records to the cash receipts. She also maintained all records of the cash receipt books. In this case, the employee segregated certain blocks of receipt numbers within the cash receipt books for her own purposes. When customers paid in cash, the receipt would either be written from one of these segregated blocks of numbers of from the end of the receipt book. When daily reconciliations of cash receipts were performed, the employee ignored these transactions for accountability purposes. Thus, more revenue was collected than deposited. There was a segregation of duties problem for this individual who had almost complete control over the market's cash receipting function for daystall rent. Attendance records were also falsified.

A Customer Service Specialist in the Secretary of States Office took $10,670 in cash received from customers when apostilles (attestation of the accuracy of a document obtained from an official government source in the United States and used by citizens to assist them in conducting business in foreign countries) and certificates were issued and when flags were sold over a three-year period. An additional $14,750 in checks received from customers could not be accounted for. Accounting records were falsified to conceal these losses from recorded cash receipt transactions. Poor internal controls prevented the Agency from fixing responsibility for these losses. Cash receipt numbers issued were omitted from the daily cash listings to the fiscal office. These transactions were for cash. When daily reconciliations of cash receipts were performed, the employee ignored these transactions for accountability purposes. Thus, more revenue was collected than deposited. While the missing receipt numbers were obvious from gaps in the numbers shown on daily activity reports to the agency fiscal office, no one monitored this important attribute about cash receipting or noticed this discrepancy. The same receipt number was issued multiple times for computer-generated cash receipts. Voids were not supported, and Rediform receipts were used. Receipts were not issued for over 250 transactions found in Agency files.

CASHIERS WHO MAKE SHORT DEPOSITS

Cashiers often initially record accountability for funds received from customers for the many and varied services provided by any entity, take cash from the till, and then make short bank deposits (amounts less than that collected). Every cashier makes mistakes, and you can't trust those who don't. But, if entities make cashiers responsible for cash overages and cash shortages, rather than officially recording them as miscellaneous income and expense, respectively, they'll make crooks out of them. Cashiers will manipulate transactions in order to balance and avoid making up known shortages. This is one of many reasons why cashiers "pre-balance" their account about an hour or so before final closing. Managers should informally monitor all overages and shortages, by cashier, to determine when circumstances exist that warrant removal of an individual from this sensitive position. The question for management officials is: "How much of a loss will you tolerate?".

Red Flags:

- Significant and unexplained daily cash shortages are noted by a particular cashier or at a specific cash receipting location.
- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.
- Revenue projection using alternative records reveals a significant decline in a local revenue source.
- Deposits are not made daily or intact.
- Cash registers are operated in an open cash drawer mode.
- Multiple cashiers operate from a single cash drawer.

Fraud Detection:

- Be observant of all activity during unannounced cash counts.
- Determine whether managers monitor the cash overages and shortages of each cashiers.
- Perform an analytical review of all local revenue sources.
- Use alternative records to verify the reasonableness of all local revenue sources.
- Analyze variances of cash overages and shortages over a selected period of time to identify any adverse trends by any particular cashier or by the entire cash receipting function.

CASE EXAMPLES

College cashiers stole $6,300 and $1,300, respectively, from tuition fees and other miscellaneous revenue sources by making short bank deposits. All transactions were properly recorded on a computer cash register system. However, at the end of the day, total cash receipts were significantly less than the amount of recorded accountability. No one was able to fix responsibility for these losses because the college regularly used multiple cashiers for a single change fund and cash register. Everyone passed lie detector tests. This entity (same one with two cases within 90 days) will tolerate up to $1,800 short per day without any further investigation. There were also 20 internal control weaknesses cited in the audit report covering only cash handling procedures.

A city treasurer stole $15,600 from cash collections over a two year period by making short deposits after recording accountability for the funds. This individual falsified entity accounting records by entering a fictitious deposit in transit on the monthly bank reconciliation to compensate for these shortages. As the amount of the fraud increased over time, so did the non-existent bank deposit in transit. Auditors missed this fraud in two successive audits by failing to confirm deposits in transit (using cash count cut-off bank statement procedures). After attending the exit conference on the second audit, an audit supervisor didn't like the sound of what he heard (i.e.; cash receipts don't equal deposits, people are making mistakes the same as last year, and be more careful in the future). This supervisor performed additional substantive audit tests and detected the fraud. Any review of the monthly bank statement and related reconciliation would have detected the fact that none of the recorded deposits in transit ever reached the bank.

A town clerk-treasurer stole $10,100 from water utility cash receipts by making short deposits after recording accountability for the funds. This is a good example of a case where the individual perpetrated more than one type of fraud at the same time. When answering the question: "What else does this person do?", the auditor determined that this individual was responsible for all cash receipt and cash disbursement functions. After further audit tests, an additional $8,400 loss was detected. This individual also wrote checks to himself and for unauthorized purposes in a cash disbursements scheme.

"FREE" ACCESS TO SAFES AND VAULTS AND NO FIXED RESPONSIBILITY

Frauds involving cash receipts often occur at entities when too many people have unrestricted access to safes and vaults, when multiple cashiers operate from a single cash drawer, or when the entity does not maintain adequate records to establish accountability for funds by specific individual. Police investigators usually administer lie detector tests to everyone involved when losses occur. A policy which fixes responsibility for funds is one which requires one cashier, one change fund, and one cash register during cash receipting operations.

Internal control procedures for access to safes and vaults and their combinations apply equally as well to computer passwords. Employee access to safes and vaults must be restricted, and combinations (or computer passwords) must be changed periodically. (Mandatory computer

"lockouts" are often used when employees do not change computer passwords within the prescribed frequency.) Combinations must not be written down in the office or given out to unauthorized personnel, and must be changed when employees terminate employment.

Most auditors believe that entity employees wouldn't deliberately lie to them. However, when asked if they write the safe or vault combination down somewhere in the office, they'll rarely, if ever, tell you that they do (even when that is actually the case). Therefore, instead of asking: "Do you write the safe combination down somewhere in the office?", use an alternate question to get the same information a different way. Ask: "Where do you write the safe combination (or computer password) down in the office?". These same employees will use non-verbal body language that gives you the correct answer to this question. They will usually look right where they have the safe combination (or computer password) written down. So, when you ask this question, look directly at them to see what they do.

Red Flags:

- Inappropriate access to safes and vaults (i.e.; unrestricted access, or too many people).
- Safe and vault combinations (or computer passwords) are not changed periodically or when individuals terminate employment.
- Unexplained cash shortages occur from safes and vaults.
- The entity does not have a policy specifying that no one will be allowed in the safe or vault alone.
- For large vault operations, the entity does not have a security system identifying the times every individual enters and leaves the vault.

Fraud Detection:

- Be observant of activities at all safe and vault locations.
- Determine whether managers change safe and vault combinations (or computer passwords) periodically or when individuals terminate employment.
- Review police reports for thefts of funds from safe and vault locations.
- Review security system reports indicating safe and vault access to determine if any individual entered the facility alone.

CASE EXAMPLES

A university was too busy to make daily deposits of tuition cash receipts during registration and experienced a $3,500 loss of funds. All funds were counted and balanced each day, but were not deposited in the bank as required. Instead, they were stored in a vault for further processing.

Three people knew the vault combination, and 21 people had unrestricted access; but, no one was reported to have had access alone. When bank deposits were being prepared three weeks later, a loss of $1,500 was noted in one day's business. The following day, a loss of $1,000 was noted in another day's business. When the deposit with the first loss was re-counted, it was short another $1,000. This proves that as long as funds are retained without being deposited, funds will disappear (often daily) as long as employees have unlimited access to them. All employees passed lie detector tests administered by the campus police. Two years later, one employee confessed to another crime, and also admitted to this theft; however, he indicated that he stole $8,000, not the amount indicated above (he wanted full credit for the crime). He worked alone during the graveyard shift and had access to the vault.

An employee in a decentralized office of a state agency stole $6,000 from the sales of fishing stamps (imprest fund). Since everyone in the office knew the combination to the safe, and 30 people had access to cash receipts, no one was able to fix responsibility for this loss. Since the safe was very old and hard to open, the safe combination was painted on the dial.

A municipal court cashier stole $4,200 from customer payments which were initially receipted at the police department, but which were never recorded in the court's records. These funds were picked-up from the police department where the court clerk signed a log evidencing the transfer of funds, but disappeared while in transit to the court. Since there were multiple people who worked in the court, and since transactions were not immediately receipted by the person who picked-up these funds from the police department, anyone in the office could have stolen these funds (no fixed responsibility). No one confessed.

A town police officer stole $9,200 from municipal court cash receipts to pay his wife's creditors from a failed business enterprise. These funds were not properly safeguarded in the court office before the bank deposit was made. They were left in an unattended and unlocked box. When shortages first were experienced, court officials took action to move (not properly secure) the unlocked box to another location within the office. Losses continued. When all employees who had access to the court facility were questioned, a police officer confessed to the crime.

NO DECENTRALIZED DIRECT DEPOSITS

Entities often insist that all decentralized cash receipting operations transmit funds to a central treasurer function before accountability is established over funds received. However, they usually do not implement the proper level of control over funds to ensure that responsibility is fixed in the event of a loss of funds (they never believe that it will happen).

If losses occur when the decentralized location makes direct bank deposits, it's relatively easy to establish who was responsible for the loss. But, when couriers are used for transmittals (using either locked or unlocked bank bags; and employees or security personnel), and when additional cashiers process these transactions (i.e.; receipt, accountability, and deposit of funds), entities leave themselves open to losses because too many people subsequently get involved in handling these funds. Too many entities use unlocked bank bags for transmittals, and have only one person count funds upon receipt. When losses occur, they are unable to fix responsibility because it's not known whether the perpetrator is the person who transmitted the funds, the courier, or the person who received the funds.

- A three-part transmittal form is required when funds are sent from a decentralized location to the central treasurer (file copy, two copies with the funds, including one copy for come-back, and one copy for the central treasurer). Two people must open, count, and receipt all funds transmitted (a copy of this receipt is then returned to the decentralized location).

- A two-part transmittal form is required when funds are hand-carried to the central treasurer (file copy and copy with funds for the central treasurer). All funds must be counted and receipted at the time of the transfer.

Red Flags:

- Unexplained cash shortages occur in the courier system for funds traveling from decentralized cash receipting locations to the central treasurer function, or from the central treasurer function to the bank.

- Only one person at the central treasurer function counts funds which have been transmitted from decentralized cash receipting functions.

- Unlocked bank bags are used to transmit funds from decentralized cash receipting locations to the central treasurer function.

Fraud Detection:

- Be observant of all activity during unannounced cash counts.

- Determine how funds are transmitted and the number of people used to count funds at each location.

- Review police reports for thefts of funds from all cashier functions.

- Agree (compare) the amount of cash receipts shown at the central treasurer function with the amount of cash receipts recorded at decentralized cash receipting locations for the same transaction or event. Use account or customer confirmations, when practical.

CASE EXAMPLES

The chief cashier of a city transit system stole $240,500 over a five year period from user fees (bus fares) which were transmitted from a decentralized cash receipting location to a central vault location prior to being deposited in the bank. The decentralized location counted and balanced each day's business, but transmitted these funds to the central vault in an unlocked bank bag. The entity made one trip to the bank each day for the central bus fare counting room deposit and all decentralized location deposits. A courier noticed that the decentralized location bank bags were relatively thin when transmitted to the central vault, but were pretty thick when transmitted to the bank for deposit. Upon receipt at the vault location, the chief cashier opened these deposit bags to determine how much money was present in large denominations ($20's,

$50's, and $100's). Since the vault was collocated with the central room where all bus fare boxes were brought for counting prior to making the overall bank deposit, the chief cashier simply made a cash for cash substitution (i.e.; unaccounted for cash from the bus fare boxes was substituted for accounted for cash from the decentralized bank deposits) in order to accomplish this embezzlement scheme. Lists of the serial numbers of large currency denominations were prepared at the decentralized location, and again at the bank. The missing currency represented the amount of funds stolen at the central vault location. The chief cashier was also filmed (by covert video camera) making these currency exchanges. At the time of his arrest, the chief cashier was stealing money at the rate of $1/4 million per year. He started taking $20 a day once a week (progressive). While no one was supposed to be in the vault alone during the day, the chief cashier did this routinely. While the transit system had a security system installed which provided a report when anyone entered the vault, this access report was distributed directly to the chief cashier (the fraud perpetrator). Therefore, it was useless.

A housing manager in a preservation and development authority stole $62,000 from hotel room rental fees and accounts receivable payments while the funds were in transit from the decentralized hotel location to the central treasurer function. This individual was acting as a courier at the time of the thefts. Some accounting records were also destroyed (hotel daily activity reports for selected shifts of work) to eliminate accountability for these funds, and some entity checks were endorsed for personal gain (forgery). The entity did not monitor operations to ensure that a daily activity report and resulting cash receipts were received for each of the 3 daily shifts at the hotel.

RETAIL SALES ACTIVITY SCHEMES

In governmental entities, retail sales activity schemes most often occur in school districts where perpetrators simply collect the money and steal it. These associated student body fund-raising revenues are public funds in some states, including Washington.

In order of frequency, these losses have been from soft drink machines, candy sales, school store operations, and other miscellaneous merchandise sales. The primary method of detection is by computing expected revenue and comparing this amount to actual revenue (i.e.; beginning inventory, plus purchases, less returns and ending inventory, priced at retail, equals expected revenue). The differences between expected revenue and actual revenue represents the amount of the loss. When no records have been retained for these retail activities, it's impossible to determine who perpetrated the crime (no fixed responsibility), or whether the loss involved inventory (theft and gifts) or money (theft and informal expenditures), or both.

Critical Path for Success in Any Associated Student Body Fund

What does "Plan For Success" mean for Associated Student Body (ASB) Fund events/activities? The following outline will help the District meet its goals and objectives:

(1) District Guidance. Ample guidance is available from the Office of the Superintendent of Public Instruction (OSPI) and the Washington Association of School Business Officials (WASBO). WASBO has a web site that includes the ASB Fund Accounting Manual, an ASB

Fund-Raising Handbook, and an Activity Coordinators Guide for the ASB. Districts should use this guidance to develop their own policies and procedures. This same information may also available from other Districts. Official policies and procedures should be approved for all ASB Fund fundraising activities.

(2) District Training. The District should provide a training class for all staff holding fund-raising activities. The key is to make sure that all staff members are aware of your way of conducting business. Clubs should not be allowed to hold a fund-raising event unless the sponsor has been appropriately trained. Each person trained should sign a certificate/agreement that they have received the training, have read the District's policies and procedures, and understand what is required of them when a fund-raising event is held (the rules) as well as what the District will do if this does not occur (the consequences). This signed certificate/agreement should be maintained on file at the District. Failure to follow District policies and procedures or opening an "off-book" bank account to handle the proceeds of a fund-raising event and inappropriate activities should be grounds for subsequent employee disciplinary action.

(3) District Centralized System of Approval and Control. Districts should have a central system to review and approve all fund-raising events each year. Events should be spread throughout the year so that the parents and community don't get over-loaded with multiple fund-raising events in a short period of time. A central focal point should be established to coordinate which clubs are authorized to sponsor specific event types by date. Students must approve all fund-raising events to be held.

(4) Staff Direction and Guidance. When a fund-raising event has been properly coordinated and approved, the District should initially provide direction and guidance to the staff to ensure that all events are managed pursuant to District policies and procedures (i.e.; plan for success). This guidance should be provided prior to the actual event and clearly indicate the District's expectations. This includes providing the specific prenumbered forms that are required to document the revenue from each event, because these forms will be different depending upon the type of event held. It also includes determining the method the District will use to appropriately document the revenue from each event. Specifically discuss this with the staff to ensure they succeed. At the appropriate time, issue a reasonable change fund for each event, as appropriate, and require the staff to sign a receipt acknowledging accountability for these funds and any other prenumbered forms associated with the event. **Planning for success is critical.**

(5) District Monitoring. After approving a fund-raising event, the District should monitor the activity from each event to ensure that it is being managed pursuant to District policies and procedures and that the District's expectations are being met. This monitoring should be continuous throughout the period of time the fund-raising event is active. The District should ensure the staff document accountability for all funds received, prepare an activity report for each fund-raising event, promptly turn-in all revenue received and obtain a receipt from the District's central treasury function, and keep copies of all documents (i.e.; receipts, invoices, reports, etc.) on file for subsequent review by the District and audit by the State Auditor's Office. **Monitoring is critical for success.**

(6) Fund Accountability Determination. At the conclusion of a fund-raising event, the District should analyze the outcome to ensure that the District's expectations were met and that the appropriate amount of funds was collected and turned-in for deposit. The District should perform a gross profits test or reasonableness test for each fund-raising event, as appropriate, to determine whether the amount of funds received reconciles with the sales of inventory and the District's initial revenue expectations. Document all variances for subsequent District review and audit by the State Auditor's Office.

Associated Student Body (ASB) Fund - Common List of Concerns

(1) **Fundraising Activities**.

- Faculty advisors managed fundraising events, but did not attend District-sponsored training classes. Perhaps the District should revise its policies and procedures to state that faculty advisors cannot conduct a fundraising event unless they have attended a training class.

- If a faculty advisor does not follow the District's policies and procedures for fundraising activities, for one or more events (discretion rests with the District), perhaps the District should revise its polices and procedures to state that such faculty advisors cannot conduct future fundraising events until such time as they have attended a refresher training class (as a consequence).

- Lost profit opportunities for retail sales events. The amount of revenue generated does not meet expectations (i.e.; unit cost x number sold = revenue). Example: Gross profits determinations were not made. There was $3,000 in lost revenue from a gold card sales event (see blended operations below). A private non-profit organization solicited sponsors for the event and purchased the cards, but the District received the revenue from the sale of the cards. A faculty advisor admitted to a police investigator that some funds from this source were misappropriated. There were no records available to prove this condition.

- Inadequate supporting documents for accounting purposes. Records do not exist or are insufficient for any meaningful conclusion to be made about the

accountability for public funds. When retail sales events are involved, there were no inventory records of the product.

- No records of transfers of accountability for products and money from faculty advisors to students, and vice versa (no fixed responsibility).

- Faculty advisors either opened an unauthorized bank account in the District's name (using tax identification number) or deposited funds collected in their personal bank account. Perhaps the District should revise its policies and procedures to state that faculty advisors cannot do these things with public money, and if detected, will face appropriate disciplinary actions (as a consequence). In some instances, all revenue collected was not deposited in the bank. The faculty advisor used whatever procedures were deemed appropriate under the circumstances to manage the funds to conduct operations in support of the school function, regardless of the District's policies and procedures for these activities. In addition to violating District policies and procedures and state law, these types of activities put faculty advisors at the risk of being accused unjustly of misappropriating public funds when that may not be the case.

- When these off-book activities occur outside the control of the ASB Fund, faculty members often spend money for unwise purposes, and net revenues and expenditures when funds collected are eventually turned-in to the District. In addition, all funds collected and accounted for in this manner are public funds.

- Faculty advisors don't always use the customer as part of their internal control system. Example: Customers sign a prenumbered cash collection sheet for revenue from car washes when they "donate" funds to the school function.

- Districts don't always understand all the rules associated with the specific fundraising activity. Thus, the revenue accountability analysis for the event is incomplete. Example: Sales of cookie dough.

    - The company's invoice to the District includes only the items ordered (and at full-box quantities). Thus, more products are usually received than ordered. These extra tubs of cookie dough must be considered in any reconciliation.

    - The company sends a separate invoice to the faculty advisor that includes the free tubs of cookie dough (one free tub for each 10 tubs sold). These free tubs of cookie dough must be considered in any reconciliation.

- The extra and free tubs of cookie dough are given as gifts to faculty advisors, staff members, students, and others associated with the event. This is a violation of the Washington State Constitution.

(2) **Student Retail Stores**.

- Obviously fictitious void transactions are indicated on detail cash register tapes.

- The gross profit margin is significantly less than normal. Some faculty advisors don't know what normal is or should be for the store. Example: Gross profit margin is 25% instead of 35% (normal, based on product lines sold), and no one noticed.

- No records of transfers of accountability for money from faculty advisors to students, and vice versa (no fixed responsibility). This includes the change fund at the beginning and end of the day as well as the revenue at the end of each day.

- Cash register "Z" tapes (total accountability) are missing (numerical counter), or document more revenue than was deposited with the ASB Fund Secretary, and no one noticed. But, the amount of the deposit exactly equals the data on the form used for accountability purposes at the end of each day at the store.
- Inadequate monitoring. The District expects the faculty advisor to monitor student activities at the store. But, no one monitors the faculty advisor or overall store operations (fatal flaw).

(3) **Faculty Advisor as Agent of the District**.

- When parents donate funds for any purpose and give the money to a faculty advisor, these funds become public money and must be appropriately accounted for and controlled within the ASB Fund. Example: Parents donated money to pay for the travel costs of students attending tournaments and other special events to keep overall costs low. A faculty advisor admitted to a police investigator that some funds from this source were misappropriated. There were no records to prove this condition.

- Faculty advisors opened charge accounts at various vendors in order to conduct purchasing activities outside the control of the ASB Fund. Perhaps the District should revise its policies and procedures to state that faculty advisors cannot conduct purchasing activities in this manner, and if detected, will face appropriate disciplinary actions (as a consequence). Sometimes the faculty advisor pays these bills, and sometimes they don't. Unauthorized awards were made, and scholarships were granted to students who were unable to pay the fee for participation in a camp. Example: A District had to protect its credit rating by

paying for a faculty advisor's purchases totaling approximately $9,500. Items purchased from these sources were often given as gifts to the faculty advisor, staff members, students, and others associated with events. This is a violation of the Washington State Constitution.

(4) **Blending of ASB Fund Activities with Other Organizations**.

- The common rule follows. When faculty advisors and students conduct fundraising activities, it's an ASB Fund event. When parents conduct fundraising activities, it's a Booster Club event. Commingling private and public funds makes the money public funds.

- Districts did not have any policies about faculty advisor participation in extracurricular activities associated with Booster Clubs and other private non-profit organizations that had similar activities to the faculty advisor's position. Perhaps the District should revise its policies and procedures to state that faculty advisors can or cannot participate in these types of organizations (discretion rests with the District), and that the District must approve any authorized participation in advance. If any unauthorized participation is detected, faculty advisors should face appropriate disciplinary actions (as a consequence).

- Districts don't always know the number of Parent-Teacher-Student-Associations or Booster Clubs that participate in community activities with them, and have not entered into any formal agreement with these organizations so that both parties understand the rules associated with conducting activities in the name of the District.

- A faculty advisor formed a private non-profit organization. The organization had purposes similar to the faculty advisor's position at the District, and the same students participated in both District and private non-profit organization activities. Additional individuals participated in only the private non-profit organization.

- Districts don't always confirm that Booster Clubs are legitimate organizations. A loosely-knit group of parents who have good intentions and appear to be conducting worthwhile endeavors does not meet the definition of a Booster Club.

- Districts should establish a file on each authorized Booster Club that participates in community activities with the District. As a minimum, the file should include at least the following information on each organization:

    - The Constitution and By-Laws.

- A current list of Officers and Directors.

- The Federal tax identification number.

- The letter of determination of tax-exempt status from the Internal Revenue Service [Section 501c(3)].

- Districts can determine whether or not an organization has officially filed its application with the State of Washington, Secretary of States Office, Corporations Division, by searching their web-site at www.secstate.wa.gov/corps by using the first word in the organization's name.

- District's actually operated a Booster Club and had custody of all accounting records for the organization, including the checking account. All funds collected are public funds under these circumstances.

- Faculty advisors, without the knowledge or approval of the District, blended ASB Fund financial activities with the operations of Booster Clubs and private non-profit organizations. The primary accounting records were maintained at the Booster Club and private non-profit organization rather than at the District.

    - Faculty advisors and students participated in both organizations when blending occurred. The events were clearly ASB Fund activities.

    - Participation in fundraising activities was used to determine the student's grade in the school class associated with the events of the organization.

    - Private fundraising activities were conducted on District property using faculty advisor time; using official e-mail for advertising, promotion, and solicitation of sponsorship; and using the copy machine.

    - A faculty advisor filed a false vendor invoice with the District to obtain payment from both the District and a private non-profit organization for the same expense.

    - A faculty advisor misappropriated approximately $5,000 from a

private non-profit organization by writing checks to pay personal bills from the checking account, using an ATM card on the checking account for cash withdrawals for personal purposes, and using the debit card on the checking account to make personal purchases.

- When blending financial activities was discussed with Booster Club Directors, one Director stated they knew something was wrong, but just did not know what to do to identify what it was. The issue became clear when the results of the audit were discussed with the Directors.

(5) **Faculty Advisor Employment**.

- When faculty advisors conduct irregular activities or activities outside the control of the District's ASB Fund, their employment with the District is often negatively affected and sometimes terminated.
- These severe consequences can be avoided with proper faculty advisor training and District monitoring of overall ASB Fund events.

Associated Student Body (ASB) Funds
What is public versus private money.
What is ASB Fund versus parent group activity.

The Washington Administrative Codes (WACs) governing associated student body and non-associated student body private monies have recently been adopted. The general rules for fund-raising activities are presented below.

References: WAC 392-138-003 – WAC 392-138-210 available at www.k12.wa.us/safs under Rules (WACs).

- Associated Student Body - Public Moneys

  - **All** ASB activities must be approved by the board of directors.
  - ASB must prepare a budget.
  - ASB is subject to bid law requirements.
  - ASB funds can **only** be used for cultural, athletic, recreational or social purposes (CARS).
  - Analysis of expected profits should be performed prior to any event/activity.
  - Reconciliation of receipts to revenues to expected profit analysis should occur following all events/activities.

- Parent Groups - Booster Club and Parent Teacher Association - Private Money

  - The school board should have policies to address the approval of activities of private groups.
  - The activities/events must be planned, managed and operated solely under the direction of the parent group.
  - When using district facilities, the group must follow district policies.
  - Funds cannot be commingled with ASB money.
  - Keep the activity an "arms length" transaction.

  Note: These groups must be official private non-profit organizations rather than "loosely knit groups of parents, advisors, or other concerned citizens.

- **Non-associated Student Body - Private Money**

  - Student groups may raise moneys through fundraising or solicitation in their private capacities.
  - Prior to such activity, the school board must approve policies defining the scope and nature of the event/activity. School board policy should include provisions to ensure appropriate accountability, including prompt deposit, holding the moneys in trust, and disbursement only for the intended purpose of the event/activity.
  - If a charitable purpose is involved, the charity must qualify. Charitable purposes do not include any activity related to campaigning for election or promoting or opposing ballot propositions.
  - Prior to solicitation of such funds, notice must be given identifying the intended purpose of the fundraiser. Further, the notice should state the proceeds are non-associated student body funds to be held in trust by the school district exclusively for the intended purposes.
  - The school district shall either withhold or otherwise be compensated or reimbursed an amount from such moneys to pay its direct costs of handling these moneys and in providing the service.
  - Moneys are to be held in trust by the school with the ASB Fund or within a trust fund, and funds must be disbursed exclusively for the intended purpose.

Internal Controls Over Retail Sales Activities

Inventory of Merchandise for Resale (Primarily School Stores)

- Secure storage facility
  - Limited access to keys to storage area(s)
    - Maintain a list of keys issued to all responsible individuals
- Maintain an inventory record showing all purchases and issues
  - Perpetual inventory record
- Take and document a periodic inventory of merchandise
- **Perform and document a gross profits test**
  - By event for specific retail sales events
  - For continuing sales activities
    - Minimum frequency is beginning and end of year
    - Preferred method is a periodic frequency for this
  - Compute as follows:
    - Beginning inventory priced at retail value
    - Plus total purchases priced at retail value
    - Minus ending inventory priced at retail
    - Equals cost of goods sold at retail
    - Compare the above amount to your revenue reports
    - Any difference represents a loss of revenue from activity
      - Lost profit opportunity
      - Perform an investigation to determine reason(s) for any unusual variance/discrepancy
      - Potential causes for any variances
        - Inventory given away? (Prohibited)
        - Cash receipts expended without properly recording the transactions? (Prohibited)
        - Other? (Obtain specific explanation)

Soft Drink Machines (Or Retail Store Operations)

- Limited access to keys to pop machine(s)
  - Maintain a list of keys issued to all responsible individuals
- There are three kinds of keys for pop machines
  - Key access to inventory only
  - Key access to cash only
  - Key access to cash and inventory
- Know whether your machine has an internal numerical counter
  - If so, reconcile inventory issues to money received
- **Always have two people collect the money from pop machines**
  - Preferably a student and an advisor
  - Never send a student or advisor alone (Temptation)
- Always have these same two people immediately count the money
- Prepare a daily activity report indicating the amount of funds
- This serves as a transmittal form from the activity to the central treasurer function

Turn-in these funds to the central treasurer immediately (**fix responsibility**)
Obtain an official prenumbered receipt for the cash turn-in from the central treasurer

Remember: Even if the District enters into a contract with a soft drink vendor, the District still must review the activity to ensure the expected revenue from the operations has been received.

Attendance Activities (Sports/Dances/Etc.)

Use prenumbered tickets (theater type by the roll)
Record beginning and ending ticket numbers
Have responsible individual sign for change fund used
Control admission/access to the facility
Safeguard funds after the event
Always have two people immediately count the money
Prepare a daily activity report indicating the amount of funds received from the event
This serves as a transmittal form from the activity to the central treasurer function
Reconcile ticket sales and cash receipts
Turn-in these funds to the central treasurer immediately (**fix responsibility**)
Drop-box at local bank (Funds to bank/Paperwork to school)
Secure storage in safe/vault at school facility
Obtain an official prenumbered receipt from the central treasurer for the funds actually turned-in

Miscellaneous Retail Sales Fund Raising Events

Use official prenumbered receipt forms
An official receipt has the entity name printed on it
Entity controls the numerical sequence for printing
Don't use "Rediform" receipts (Good form, just not for public money)
Can be purchased anywhere by employees
One for you and one for me recording of events
No entity control over numerical sequence
Ensure mode of payment is indicated on form (Cash or check)
Centrally purchased
Centrally warehoused/issued
Record who gets which books of receipts
Monitor sequential use of receipts from each source
Always have two people immediately count the money
Prepare a daily activity report indicating amount of funds
This serves as a transmittal form from the activity to the central treasurer function
Turn-in these funds to the central treasurer immediately (**fix responsibility**)
Obtain an official prenumbered receipt from the central treasurer for the funds actually turned-in
Each entity must monitor activities to ensure that funds are routinely

turned-in from all continuous revenue sources

Other Retail Sales Activities

These above principles apply to all other types of retail sales activities also
- Number of activity cards issued times cost equals revenue
- Number of drivers education students times student cost equals revenue
- Number of school annuals issued times selling price equals revenue

School officials must perform reasonableness tests for revenue from all revenue generating activities (analytical procedures)

This list is not intended to be all inclusive

It's a good start in the right direction

Critical to any system of internal control procedures is a written record (i.e.; a policies and procedures manual or document)

If you don't tell your employees what you want and expect, you won't always achieve the correct or desired results (plan for success)

If you don't know where you're going or why, then any road will get you there. But, it might not be the right road. And, you might even experience fraud along the way. Certainly not a desirable event!

TRAINING EXAMPLE

A case example follows this section which explains the computation process for a typical retail sales loss of funds case. For ease in presentation and understanding, this example is based on an item of resale merchandise whose cost is $1, and whose retail sales price is $2. This example depicts an item with a 100% markup. It's cost represents 50% of the sales price. While not used in the example, actual merchandise data is also shown for soft drinks and candy. This information is presented purely for information purposes.
The example has a beginning inventory of $1,000, purchases of $10,000, an ending inventory of $2,000, and a cost of goods sold of $9,000. In this example, the retail value of these goods would be $18,000 (100% markup).

Based upon this example, four different cases are presented. The only variable in the equation is the amount of revenue actually received by the retail sales activity. In each of these cases, both the "net income from sales" and the "loss of funds" have been computed. Case number 4 is the only proper retail sales activity. The other 3 cases represent losses of funds in varying degrees.

One of the interesting things that leaps out of this example is that a retail sales activity can make a profit (net income), but still incur a loss of funds. Many people find this concept hard to understand. They believe that everything is just fine if any profit has been made. After reviewing this example, this should not include you.

For audit report purposes, these losses are always presented at the maximum amount possible. This represents the cost of goods sold at "retail" value. This means that the loss of funds is presented as a 100% cash loss.

For the purposes of settlement, insurance bonding companies want the loss presented at the minimum amount possible. Therefore, they want to present the loss as a 100% merchandise loss. This represents the cost of goods sold at "cost" value. In the example cited, this merchandise loss amount is 50% of the cash loss amount. However, one thing about this example is certain. The merchandise loss amount represents the actual amount of expenditures made for purchases of merchandise for which nothing was received in return (not a single penny). This should make it very clear that we're dealing with a real loss of funds in these cases rather than a hypothetical loss of funds, as many people would suggest or like to have you believe. Money was invested in inventory which generated no revenue. Certainly, this is not the way to manage a retail business!

So, based upon the differences in the presentations above (i.e.; retail versus cost), it's easy to understand why insurance bonding companies want to start negotiating the amount of the loss where they do. They immediately take the audit loss amount and cut it in half. In reality, all settlements should be made somewhere between this minimum loss amount (all merchandise) and the maximum loss amount (all cash). The average settlement amount has been about 75% of the loss amount included in our audit reports. Settlements are reached on these terms because it's not cost effective to try to obtain additional amounts through civil litigation. But, in many cases, insurance bonding companies have an exclusionary clause which precludes coverage for "lost profit opportunities". In this case, retail sales losses of this type cannot be recovered from insurance bonding companies.

RETAIL SALES ACTIVITY LOSS OF FUNDS CASE
ASSOCIATED STUDENT BODY FUND

MERCHANDISE DATA

	COST	MARKUP	SALES PRICE	% OF MARKUP	COST AS A % OF SALES
AUDIT EXAMPLE	$1.00	$1.00	$2.00	100%	50%
SOFT DRINKS	.27	.23	.50	85%	54%
CANDY	.29	.11	.40	38%	73%

AUDIT EXAMPLE:

	AT COST	AT RETAIL
BEGINNING INVENTORY	$ 1,000	$ 2,000
PLUS: PURCHASES	10,000	20,000
TOTAL INVENTORY	$11,000	$22,000
LESS ENDING INVENTORY	(2,000)	(4,000)
COST OF GOODS SOLD (GOODS AVAILABLE FOR SALE)	$ 9,000	$18,000

COMPUTATIONS:

(1) INCOME STATEMENT

		CASE NO.1	CASE NO.2	CASE NO.3	CASE NO.4
SALES REVENUE	(RETAIL)	$ 9,000	$12,000	$15,000	$18,000
LESS: COST OF GOODS SOLD	(COST)	(9,000)	(9,000)	(9,000)	(9,000)
NET INCOME FROM SALES		$ 0	$ 3,000	$ 6,000	$ 9,000
COST AS A PERCENT OF SALES		100%	75%	60%	50%

(2) LOSS OF FUNDS

SALES REVENUE	(RETAIL)	$ 9,000	$12,000	$15,000	$18,000
LESS: COST OF GOODS SOLD	(RETAIL)	(18,000)	(18,000)	(18,000)	(18,000)
LOSS OF FUNDS (MAXIMUM/RETAIL) (100% CASH LOSS)		$ 9,000	$ 6,000	$ 3,000	$ 0
LOSS OF FUNDS (MINIMUM/COST) (100% MERCHANDISE LOSS)		$ 4,500	$ 3,000	$ 1,500	$ 0

Red Flags:

- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.
- Revenue projection using alternative records reveals A significant decline in a local revenue source.
- Management does not perform periodic reasonableness tests for retail sales functions.
- Inventory records are not maintained for retail sales merchandise.
- Retail sales merchandise is not adequately safeguarded in storage.

Fraud Detection:

- Perform a reasonableness test for all retail sales activities.
- Review retail sales merchandise storage and issue controls, and inventory procedures.
- Perform an analytical review of all local revenue sources.
- Use alternative records to verify the reasonableness of all local revenue sources.

CASE EXAMPLE

Of the 294 school districts in the State of Washington (where associated student body fund-raising revenues are public funds), an average of 8 districts per year experience a retail sales loss of $6,800 each ($54,400 annually). Retail sales activity losses primarily occur in school districts where a single person controls the entire financial operations of the associated student body. Students and advisors turn-in revenue from a variety of fund-raising sources to the central treasurer without counting the money when the exchange occurs, and without obtaining a receipt for the transaction. Revenue from soft drink machines is a good example. School districts routinely send one student out to the machines to both replenish the stock and remove the money (two people should be required to do this). This individual places the money in a cloth bag, returns the funds to the central cashier function, and leaves the money in a vault. The amount of revenue from this source is exactly what the cashier at the central treasurer function says it is when it's counted, receipted, and deposited in the bank at a later date. This cashier is one of the most dangerous people in the State of Washington (high risk environment).

CHECKING ACCOUNT SCHEMES

Since bank employees deal with entity employees frequently, they often forget what they're doing and treat the entity's bank account the same as they would a personal bank account for the individual (blind trust). The following schemes occur on the cash receipts side of checking accounts:

Unauthorized check conversions. Employees endorse checks initially made payable to the entity. There are often two endorsements shown on the back of these checks. The entity name is usually listed first, followed by the individual's signature (on behalf of the entity). This is not the case when the person issuing the check leaves the payee line blank.

Unauthorized withdrawals. Employees make unauthorized cash withdrawals from bank deposits.

Red Flags:

- Irregular check endorsements on transactions between functions of the same entity (checks for transactions from customers will not be available for review).
- Decline in funds from a local revenue source from one accounting period to another.
- Complaint from entity that expected revenue from another source is missing or did not arrive on schedule.
- Amount of deposit shown on bank statements does not agree with daily activity report total.
- Copies of bank validated deposit slips are not retained on file (carbon copies only).

Fraud Detection:

- Be observant during reviews of monthly bank account reconciliations and check endorsements.
- Perform an analytical review of all local revenue sources.
- Use alternative records to verify the reasonableness of all local revenue sources.
- Review bank deposit slips for any unauthorized cash withdrawals.

CASE EXAMPLES

A chief of police at a small city and a commissioner of a water district stole $2,000 and $1,000, respectively, by cashing checks at a local bank which were made payable to the entity. These checks were endorsed with the name of the entity followed by the signature of the employee. The chief of police stated that he cashed checks to obtain change for the municipal court (not true). The commissioner of the water district stated that he cashed checks to make emergency repairs. No supporting documents could be found for these reported disbursements.

A temporary staff person working in a county mail-room facility stole $3,800 be intercepting two state warrants destined for a governmental entity, altering the payee line by typing her name above the entity's name, and endorsing the warrants to convert these funds to personal use (deposited them into her own personal bank account).

An accounting clerk at a fire district stole $8,000 by cashing checks at a local bank which had been made payable to the governmental entity. These checks were endorsed with the name of the entity followed by the signature of the employee. This clerk also made unauthorized cash withdrawals from entity bank deposits.

ESTABLISHING BOGUS ENTITY CHECKING ACCOUNTS

Employees often establish bogus entity checking accounts without the knowledge or approval of the governing body. These accounts are established to facilitate the conversion of official entity checks to personal use. All disbursements from these accounts are made payable to the employee.

Red Flags:

- Analytical review indicates a decline in a local revenue source from one accounting period to another without any reasonable explanation.
- Revenue projection using alternative records reveals a significant decline in a local revenue source.
- An inquiry is received from a bank regarding an unknown entity bank account.

Fraud Detection:

- Perform an analytical review of local revenue sources.
- Use alternative records to verify the reasonableness of all local revenue sources.
- Make an inquiry at all banks in the local area for a list of all accounts in the name of the entity, when practical.

CASE EXAMPLES

A secretary in an irrigation district stole $54,300 in cash receipts over a nine year period by depositing official entity checks into a bogus bank account. Every penny of local revenue received by this entity was stolen, including funds from: (a) the sale of timber and land; (b) the settlement of a lawsuit; (c) grants; (d) water sales and assessments; and, (e) other miscellaneous revenue. The secretary established the bogus bank account without the knowledge or approval of the district by signing the bank signature card, taking the signature card home, and then forging the signature of one of the members of the governing body. All check disbursements from the account were signed by the secretary, and all funds were used for personal purposes. There was no system of internal control because one person acted with absolutely no management review or oversight in the cash receipt and cash disbursement functions of this entity. She stole an additional $191,700 in a cash disbursements scheme by issuing prenumbered checks for claims payments to 20 fictitious companies ($163,800) and for payroll to fictitious employees ($27,900).

A building inspector in a county stole $3,100 in cash receipts over a two year period by depositing official entity checks into a bogus bank account. The building inspector established the bogus bank account using a name which sounded similar to the county's name (i.e.; "XXXX" County Building Inspection Services). This account was totally under his control. All check disbursements from the account were used for personal purposes.

An employee in a school district stole $51,700 in insurance premium payments using two methods and deposited these funds into several bank accounts under her control. Customer checks for insurance premium payments that had been made payable to the entity were removed from the district, fraudulently endorsed, and deposited into these bank accounts. She also stole entity checks which had been issued to various insurance companies and deposited them into these same bank accounts. All check disbursements from these bank accounts were then used for personal purposes.

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

Cash Disbursement Fraud Schemes

- General Accounting Office Report on Fraud
- Accounts Payable/Cash Disbursements Fraud Concepts to Remember
    - Case Study: Washington State Liquor Control Board
- Employees Issue Prenumbered Checks to Cash, to their Personal Business, or to Themselves
    - Case Study: Lake Washington School District
    - Case Study: Seattle School District (SPICE Program)
    - Case Study: Department of Fish and Wildlife
- Employees Issue Blank Checks to Themselves
    - Case Study: Public Utility District No. 2 of Grant County
- Employees Issue Prenumbered Checks to Fictitious Companies
- Caseworkers Who Process Fictitious (or Duplicate) Authorizations for Service in Public Benefit Programs
    - Computer-Related Fraud in Government Agencies: Perpetrator Interviews
- Retirement System Schemes
- Payroll Schemes
    - Concepts to Remember About Payroll
    - The Five Most Common Payroll Fraud Schemes
    - Case Study: Harborview Medical Center
    - Case Study: University of Washington Medical Center
    - Payroll Fraud Cases
    - Payroll Analytical Procedures and CAATs
    - Other Payroll Attributes and Audit Tests
- Electronic Funds Transfer Schemes
- Unmonitored Personal Service Contract Schemes
- Employees Manipulate, Misuse, or Abuse Miscellaneous Entity Disbursements
    - Assets and Personnel
    - Credit Cards
    - Telephone
    - Travel
        - Internal Controls for Travel
        - Typical Travel/Petty Cash/Time Card Fraud Scenario
        - Travel Fraud Cases
- Unauthorized Conversion of Duplicate Checks
- Stealing and Converting Blank Check Stock

GENERAL ACCOUNTING OFFICE (January 1993)
LIST OF AGENCIES MOST LIKELY TO SUFFER FROM FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

(1) Farmers Home Administration: $7.6 Billion in farm loan defaults.

(2) Department of Education: $3.6 Billion in student loan defaults.

(3) Federal Deposit Insurance Corporation: $7 Billion bank insurance deficit.

(4) Resolution Trust Corporation: $112 Billion savings and loan bailout.

(5) Pension Benefit Guarantee Corporation: $17.9 Billion in under-funded benefits for insured pension plans.

(6) Department of Health: Billions (10% of total program costs) in fraudulent Medicare claims.

(7) Department of Defense: Weapons systems acquisition involves Billions in commitments without proof systems will perform.

(8) Department of Defense: Overpricing by contractors in $150 Billion program.

(9) Department of Energy: Widespread mismanagement of $19 Billion in contracts.

(10) Environment Protection Agency: Superfund recovery of only 10% of $5.7 Billion in clean-up expenses from those responsible.

(11) National Aeronautics and Space Administration: Vulnerable to mismanagement of $13 Billion budget due to unrealistic planning.

(12) Department of Defense: $40 Billion in excess supplies in inventory.

(13) Internal Revenue Service: $111 Billion in uncollected taxes.

(14) Customs Service: 84% of trade law violations for imported cargo undetected.

(15) State Department: Over 10,000 overseas real properties (owned/leased) have history of mismanagement.

(16) Federal Transit Administration: $36 Billion in mass transit grants misused by recipients due to ineffective oversight.

(17) Department of Justice and Customs Service: $1.9 Billion in seized property inventories improperly cared for and cash not kept in interest bearing accounts.

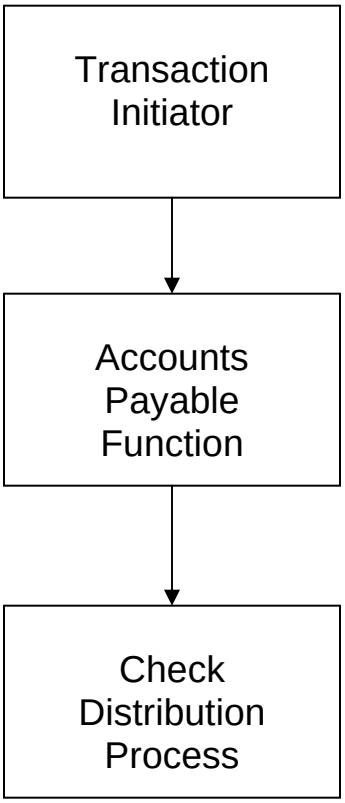
ACCOUNTS PAYABLE/CASH DISBURSEMENTS FRAUD CONCEPTS TO REMEMBER

The Subtle Compromise of the Accounts Payable System

Managers and auditors should always look for a straight line from transaction initiator to accounts payable to check distribution process in the accounts payable system. This same principle also applies in the payroll system except that the straight line is from the source (the individual) to the approval point (the supervisor) and then to the payroll function for payment. But, the fraud illustrations are slightly different.

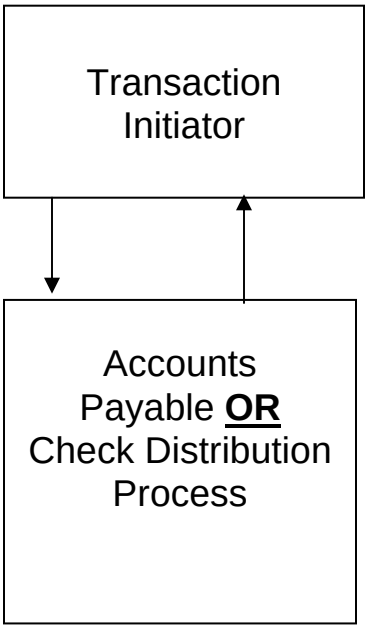
Normal Practice

(The Straight-line)



Irregular Practice

(The U-turn Concept)



The Washington State Auditor's Office experienced five significant fraud cases from January 1, 1996, through December 31, 2002 (seven years) that involved subtle compromises of the accounts payable system resulting in losses totaling $1,430,271. This presentation includes the learning objectives from these fraud cases.

Problems:

(1) The ultimate objective of any cash disbursement scheme is to obtain a negotiable instrument and subsequently convert it to cash for personal gain. Managers often think that the check issuance process is unimportant. After all, it's just paper.

(2) The largest fraud schemes involve either accounting functions being performed in the data processing function (or some other function), or vice versa. This deviation from the normal segregation of duties for personnel in these key functions lies at the heart of the most devastating cash disbursement fraud cases.

(3) Employees with too many duties are able to compromise the organization's internal control structure in the accounts payable system. When this happens, the individual usually obtains both input and output responsibilities, the "kiss of death" in cash disbursement fraud cases). Thus, they are able to create fictitious disbursement transactions using either legitimate or false vendors, obtain the check and then use the proceeds for their own personal benefit.

(4) The most common compromise of the accounts payable system is the use of "post-it notes". Employees initiating these transactions use "post-it notes" to ask accounts payable to return the warrant/check to them after issuance, usually so that they can hand-carry it to the vendor during a subsequent meeting.

(5) Managers should look for a "straight line" from the source requesting payment for the transaction, to accounts payable for review and production of the warrants/checks, to the individual making distribution of the warrants/checks. Anytime there is a "U-Turn" in the accounts payable function and the warrant/check is returned to the source, the transaction automatically becomes an exception transaction requiring intense scrutiny and monitoring by managers.

(6) The largest fraud case in the state's history ($839,707) was issued at the Liquor Control Board (LCB) in August 2002. This case involves over-billings by a freight vendor who delivered liquor from the central warehouse to the various liquor stores throughout the state. These transactions included inflated weights for deliveries, fictitious deliveries, and duplicative billings of deliveries. Of the $1,100,000 in vendor billings, almost 76 percent of all transactions were fictitious. But, an employee on the inside compromised the LCB's accounts payable system. This system compromise can happen anywhere.

Solutions:

(1) Review access controls to ensure that no employee can initiate disbursement transactions, release the batch of transactions to request production of checks, and then pick-up or obtain the negotiable instruments.

- Washington State Gambling Commission (Business Operations Section) ($71,750)

- Department of Fish and Wildlife ($137,467)

(2) Any compromise of the accounts payable system should be documented on an exception record to identify the universe of all transactions processed outside normal parameters. These include the use of "post-it notes" or any other verbal or written messages to accounts payable personnel or check distribution personnel, and picking-up checks when this is not the organization's normal procedure. Managers should periodically review the supporting documents for these transactions for trends, and examine the bank endorsements on the checks for validity.

- Liquor Control Board (Accounts Payable Vendor Overpayments) ($839,707)

- Department of Fish and Wildlife ($137,467)

- PUD No. 2 of Grant County ($236,925)

(3) Use of "pseudo vendor codes" (i.e.; one-time payments in lieu of establishing valid vendor codes) should be documented on an exception report. Managers should periodically review the supporting documents for these transactions for trends, including any abuse of the system such as multiple payments to the same vendor. We often forget that employees assigned specific computer tasks can always perform the task, at any time of the day or night, whether the action is authorized or not. The ultimate question is whether all such transactions are authorized, approved and properly supported.

- Washington State Gambling Commission (Business Operations Section) ($71,750)

- Department of Fish and Wildlife ($137,467)

(4) Prohibit either accounting functions from being performed in the data processing function, or vice versa. Accounting department personnel should not have the authority to make computer software changes to any program, such as the check redemption software program. In addition, accounts payable duties should not be performed by anyone outside the accounts payable function.

- PUD No 2 of Grant County ($236,925)

- Liquor Control Board (Accounts Payable – Vendor Overpayments) ($839,707)

(5) Ensure managers/governing boards closely monitor all disbursement transactions initiated by anyone working in the accounts payable function or by an individual totally in control of the disbursement function in a small organization, such as an executive director or financial officer, to ensure that all such transactions are properly authorized and supported and are for official purposes.

- Governor's Industrial Safety and Health Advisory Board & Washington Substance Abuse Coalition ($144,422)

- Department of Fish and Wildlife ($137,467)

(6) Ensure managers closely monitor all refund transactions disbursed by check to ensure that all such transactions are properly authorized and supported and are for official purposes. These types of transactions represent "negative cash" and are inherently high risk for fraud.

- Washington State Gambling Commission (Business Operations Section) ($71,750)

(7) Examine vendor contracts in cases where the transaction analyses or analytical review procedures suggest high, increasing, or unusual volumes with specific vendors. For example, sort all expenditures by vendor by accounting year and list them from highest to lowest dollar amount. Compare the current accounting year to the prior accounting year for unusual or unexpected variances. If something appears out of the ordinary, find out why by obtaining an explanation from management officials and then making your own professional judgment about the condition. If this is the type of vendor that is selected by some type of competitive bidding process, review the underlying contract selection file to determine if there are valid documents in the file. If not, find out why. If so, determine if the selection process was documented properly and appears to be reasonable.

- Liquor Control Board (Accounts Payable – Vendor Overpayments) ($839,707)

Washington State Liquor Control Board -- $839,797 Loss (07/01/99 – 02/28/02)

A freight vendor over-billed the Board and received at least $839,707 in unauthorized payments for 2.5 years. The vendor billed the Board for inflated weights on legitimate deliveries, billed the Board for deliveries that did not occur, and double billed for some deliveries. In addition, the vendor did not bill the Board for 382 legitimate deliveries valued at $67,843. Vendor over-billing losses are not covered by the Board's insurance bonding policy. The vendor ceased making freight deliveries for the Board in March 2002. No federal funds were involved in this case.

The Scheme: The vendor submitting false billings as indicated below.

Description	**Amount**
Inflated weights on legitimate deliveries. The vendor inflated 600 of 1,103 deliveries by over 5,000 pounds (i.e.; 54.39% of all deliveries).	$123,161.12
Deliveries that did not occur. The vendor submitted 1,100 invoices reporting 1,370 deliveries that did not exist.	600,527.84
Double billing. The vendor submitted invoices for 238 deliveries that had been previously billed to and paid for by the Board.	116,017.94
Total Losses	839,706.90
Unbilled legitimate deliveries. The vendor did not bill the board for 382 legitimate freight deliveries. We reduced the amount of loss by this amount.	(67,843.31)
Net Loss	$771,863.59

Detection Method: An employee at the Board reported to management that she had a relationship with the freight vendor and unwittingly aided in processing the unauthorized payments.

Internal Control Weaknesses:

- The review of vendor billings was inadequate. An employee, assigned to a position outside the freight vendor payment process, received and approved the vendor's billings for payment. At times, this employee also personally delivered payment warrants to the vendor. These actions compromised the Board's internal controls over freight vendor payments.

- The vendor was not required to submit original bills for payment. The vendor submitted bills by facsimile machine and was not required to subsequently provide original copies of these documents to the Board. This enabled the vendor to submit duplicate copies of bills for payment.

- There was no requirement for the staff to verify reported deliveries or the reported weights of those deliveries from vendor billings to other agency freight shipment records prior to payment. This enabled the vendor to bill the Board for shipments that were not delivered to liquor stores and for inflated weights of the deliveries.

Recommendations:

- We referred this case to the Thurston County Prosecuting Attorney and Executive Ethics Board.

- We recommended the Board seek recovery of the $771,863.59 in freight overpayments and related audit/investigation costs of $31,307 from the vendor, and improve its system of internal control to protect public assets from loss.

Sentencing: The vendor was sentenced to 57 months in the state penitentiary for this crime, the maximum length of time permitted by law.

General Disbursements.

The **voucher authorization and approval process** (accounts payable clerk, auditing officer, and governing body approvals) is the strength of the cash disbursements system in state agencies and local governments. The auditing officer function serves as an outstanding review mechanism for entity disbursements, as long as the auditing officer is at the proper level within the organization and the review is performed with interest. The approval function by the governing body can be perfunctory because members are not necessarily trained regarding what they should be looking for or the purpose of their actions. Approval of general disbursements by the governing body is not a guarantee of transaction validity.

Interim transactions and manual additions to warrant registers are high risk. These manual transactions may be shown as pen and ink changes to computer generated warrant registers, may be omitted entirely, or may represent duplicate warrants previously processed through the system. These transactions may not receive the same level of care in the authorization and approval process. The governing body may not have even approved these transactions.

Storage and issue controls over warrants must be appropriately maintained. Blank (unnumbered) warrants are high risk and require an even greater level of security than prenumbered warrants. Negotiable instruments (warrants and checks) are being stolen and redeemed without the authorization and approval of the entity. Use locked storage facilities and limit the number of employees who have access. Monitor the inventory of negotiable instrument stocks. Maintain logs for negotiable instruments issued. Promptly note sequence breaks from one run to the next. Act promptly with a "stop payment action" when numbers are missing. Determine whether an investigation is needed or if a police report should be filed.

At the heart of every fraud is a **missing or fraudulent** (falsified or altered) document. Don't use the **FIDO** concept (i.e.; "forget it, drive on". If you can't find the document supporting the transaction, your test fails. Find the right answer instead. The document may just be out of file for some legitimate purpose or reason.

Most cash disbursement frauds employ **common and simple methods**. Engage the mind and use your experience. Common sense is your most valuable resource. Since normal expenditures are repetitive in nature, scan the warrant register for suspicious transactions by concentrating on variances from the norm. Review disbursements for fictitious

vendors, duplicate payments, overpaid employees, and payments to "cash" or financial institutions. For false vendors, compare like data elements from the personnel/payroll system to vendor files. Review invoices for Rediform documents, prenumbering (make sure you don't get all the numbers, as in the only customer), post office box addresses only, lack of telephone numbers, etc. Compare the amount, payee, and endorsement on redeemed warrants to the actual warrant register for a specified period of time (block sample). Multiple endorsements are high risk documents.

The **accounting entry for cash disbursement fraud** is debit expense, assets, revenue, liabilities or fund balance and credit cash.

Since cash disbursements fraud is recorded in the accounting system, and since the attributes of concern are "**what's too high or what's too much**". Cash disbursements fraud is concealed in accounts with **high volumes** of activity and/or **high dollar** amounts. Awareness of these fraud indicators is the key to fraud detection, and detection is everyone's job. Therefore, a comparative analysis of expenditures should look for these key elements within each entity.

Fraud perpetrators are unpredictable as to position and background. They change over time with the internal control system – **the "chameleon" effect**.

It's difficult to distinguish original documents from **false original** documents. The critical element is whether or not the service was actually received.

The accounts payable function should never pay an invoice that has not been authorized and approved by the recipient of the goods and services. There are some companies that exist solely for the purpose of sending **fictitious billings** to unsuspecting organizations, simply hoping the organization will pay the bill without researching the transaction.

Pay from **original source documents** only. Do not pay from Xerox copies of documents. While facsimile documents are "original" documents under the law, and are often needed to make urgent payments, always require the vendor to mail you a copy of the original document. The original document should then be filed with the supporting documents for the expenditure.

Question vendor invoices that **do not have a street address** (i.e.; post office box address only) or a vendor who is **not listed in the telephone book**.

Make sure that all supporting **documents are valid** and represent actual purchases of goods and services. Watch out for "**cut-and-paste**" documents where all the detail is missing from the transaction. If an employee has to write the description of the item purchased on the receipt, it's a high risk transaction. Determine if the receipt submitted for reimbursement purposes is the actual receipt type issued by the vendor involved. Confirm validity if necessary. And, never accept a receipt without appropriate vendor information recorded on the document. Watch for **numerical sequencing** of receipts or invoices used for reimbursement purposes.

Identify documents that serve the same purpose as **blank checks**, such as petty cash documents, travel vouchers, and time cards. Look for **a straight line** from source to approval to payment. Eliminate the use of blank lines on these forms by crossing them out after the last item for approval. All fraud is after approval by a manager.

Don't accept the first plausible explanation for exceptions found, and make sure that an **independent party** analyzes and researches all complaints (customer feedback). The first defense is things are a mess here (by design when fraud occurs), it's an accounting problem (whatever that means), it's miscoded, or you simply just don't understand (the problem is that you do). Test all answers received. Be from Missouri, the "show me" state. Show me a transaction which when processed correctly will create this condition. There are none for fraudulent transactions.

Computer frauds are no different than manual frauds. Sometimes the only difference is that the records are maintained on computer storage media (i.e.; disks, drums, etc.) rather than in filing cabinets.

Checking Accounts/Imprest Funds.

The number one fraud in the United States, and probably the rest of the world for that matter, is the huge risk that exists today for a fraud scheme that involves the issuance of "bogus" checks by individuals outside the government. So, what can be done about this menace.

The Check Fraud Risk - Bogus Warrants and Checks.

It's important for all public entities to understand the risk posed by bogus warrants and checks. Warrant and check fraud in the United States is a $16 billion industry that is growing at the rate of about $1 billion per year. Our clients are informing the State Auditor's Office that counterfeit warrants and checks have been presented to their bank for payment almost every business day.

Producing bogus warrants and checks is a rather simple and unsophisticated process. Anyone with a few thousand dollars in computer and peripheral equipment can produce high-quality bogus documents. And it doesn't take more than a day to recover this initial investment. The perpetrators only need your bank account number, and this information is provided on every warrant and check issued. Bogus electronic debit transactions can also be created.

Banks have accepted responsibility for most of the losses resulting from these fraud schemes because public entities have promptly detected the bogus warrants and checks during the independent party bank reconciliation process. In some cases, banks have detected the counterfeit warrants and checks when presented for payment.

In response to this risk, many public entities have established either "positive pay" or "reverse positive pay" at their banks. This is a daily reconciliation of the warrants and checks issued versus the negotiable instruments being presented for payment. While both of these systems work, positive pay is the preferred method of choice, even though it is

the more expensive of the two options. An organization may also accomplish this reconciliation by using its on-line banking capability.

- Positive pay. This is an automated service provided by banks to detect bogus warrants and checks. It is extremely effective when the entity sends specific information to the bank on days when warrants and checks are issued. The bank compares the documents that come in by number and amount to a file of documents issued by the entity. If the bank has no in-file match, it contacts the entity to determine the negotiable instrument's authenticity. Two days are usually allowed for this process, but the process works better if the review is performed immediately. Counterfeit warrants and checks are then returned unpaid.

- Reverse positive pay. This method allows the entity to conduct its own daily matching procedures. Most banks offer customers a daily transmission of paid items that can be compared with the entity's issued warrant and check file. The entity must promptly research each suspicious document and advise the bank of items to be returned.

If a public entity warrant or checking account becomes the target of a fraud scheme in the private sector, the Fraud Department at Equifax, a check guarantee company, can also put a hold on the account. The company can be reached at 1-800-337-5689. The local law enforcement agency should also be contacted. Closing the bank account is another option.

The State Auditor's Office takes this issue very seriously and wants to make sure that all public entities understand the risk from bogus warrants and checks. For example, two cases have been reported where legitimate vendors created warrants for an employee purchase and a delinquent loan payment.

To counter these threats, public entities must ensure that an independent party performs the bank reconciliation in a timely manner. And, this employee should receive the bank statement directly from the bank, unopened. If bogus documents are not identified promptly, the entity will suffer a needless loss of funds. Entities must:

- Notify the bank of bogus **warrants** within **24 hours** of redemption. One public entity has suffered a $45,000 loss because one of three bogus warrants presented was not promptly identified. Another public entity identified three bogus warrants promptly and avoided a $450,000 loss.

- Notify the bank of bogus **checks** within **30 days** of the bank statement date. However, performing the bank reconciliation immediately upon receipt is preferred. One public entity has already suffered a $26,000 loss because bogus checks were not promptly identified. Two additional schemes were quickly foiled when a public entity and its bank identified a $300,000 bogus check that an individual was attempting to cash, and a bogus check where the amount has been falsely increased from $18 to $4,500.

- Ensure that your warrant and check stock is designed to meet industry standards and has a sufficient number of security features that make counterfeiting more difficult.

How people obtain a public entity's routing and bank account number is critical to understanding the problem. Every warrant and check a public entity issues provides all the information an individual needs to begin a bogus warrant or check fraud scheme. This same information can be obtained from improperly discarded trash. Unscrupulous individuals have even been known to pay people for allowing them to optically scan warrants and checks with hand-held devices at or near check-cashing facilities.

We recommend all public entities:

- Require an independent party reconcile warrant accounts daily and checking accounts immediately upon receipt of the bank statement.

- Include either positive pay or reverse positive pay procedures in banking agreements.

- Ensure warrant and check stock is designed to meet industry standards and has a sufficient number of security features that make counterfeiting more difficult.

Automated Clearinghouse and Electronic Fund Transfers.

A public entity's bank account information can also be used to create **either bogus debits or bogus electronic fund transfers**. We recently received notice about two cases in which these new methods of compromising bank accounts were used. The activity in some bank accounts is by check only. In others, the activity is by electronic fund transfers only.

The Uniform Commercial Code does not cover these transactions. These transactions are final within **24 hours** and are covered only by the underlying rules and regulations of the National Automated Clearinghouse Association.

We recommend all public entities notify the bank to filter or block irregular transaction types from their warrant, checking and savings accounts, either totally or selectively.

We recommend all Office staff emphasize the information contained in this FYI to all public entities during entrance and/or exit conferences.

References:

- Revised Code of Washington (RCW) 40.14.010/060/070, and 40.20.020
- Local Government General Records Retention Schedule (GS50-03B)
- State Auditor's Office (SAO) Bulletin No. 015

These references state that local government checks and warrants are official public records and must be retained by issuing local governments for six years from the date of issue. The retained record may be either the paper negotiable instrument or a CD-ROM of the instrument.

- RCW 43.09.185
- SAO Bulletin No. 1999-03

These references require state agencies and local governments to notify SAO of suspected or known losses (funds and assets) and illegal acts.

- Uniform Commercial Code.
- National Automated Clearinghouse Association Rules and Regulations.
- Frank W. Abagnale's Check Fraud Bulletin, 1-800-237-7443.

These references provide background information on the rules and regulations governing the processing of warrants, checks, automated clearinghouse transactions, and electronic funds transfers. They also cover the dangers of check fraud and the many remedies available to any organization when addressing this risk.

Bank Account Reconciliation. All types of **checking accounts** are high risk. The reimbursement voucher processed for all types of imprest funds (i.e.; advance travel, purchasing, petty cash, etc.) should be carefully reviewed. Appropriateness of the expenditure made for the activity involved should be clear. Employees must be alert for false (fictitious) or altered (forged) documents. While performing the monthly bank account reconciliation, you should:

Look first for **"bogus"** checks that you did not issue. These are the ones the check production mills produce using your stolen checking account number. For checking accounts, the account holder has 30 days from monthly bank statement date to notify the bank of fraudulent activity. Don't wait. Perform the reconciliation immediately after receipt of the statement.

Scan the deposit and disbursement activity of imprest fund accounts for money laundering activities, such as:

Depositing unrecorded revenue checks into checking accounts, indicating a laundering of misappropriated checks in order to obtain the proceeds for personal benefit.

Writing checks to "cash", "blank", self, a financial institution (for a money order or cashiers check), or a fictitious vendor (paying personal bills).

Making 'cash back" withdrawals from bank deposits.

The ultimate objective of any fraud scheme is to get the check, cash it, and then use the money for personal purposes.

Someone independent of the custodian must perform the monthly bank reconciliation timely and review all canceled/redeemed checks for any irregularity (forgery/alteration). This independent party should receive the unopened bank statement directly from the bank.

Comparison of check payee and amount to the check register and **review of the check endorsements** is essential. Critical steps include investigating:

Dual signature endorsements indicated on payroll checks.

Check endorsements made payable to third parties.

Check endorsements for multiple vendors with unexplained similarities.

Out-of-town checks cashed or deposited locally.

Voided checks that subsequently clear the bank (retain and file voids).

Checks issued to individuals for large, even amounts.

Abbreviated payee names (IBM/UPS), which can be easily altered.

Any other unusual check attribute determined by experience.

Review supporting documents for imprest fund reimbursement transactions for propriety. Items of concern include:

Use of original source documents only or use of falsified (i.e.; "cut and paste") documents in the file.

Validity of supporting documents.

Appropriateness of supporting documents for entertainment and meals. Budgeting, Accounting and Reporting System (BARS) Manual requirements include a list of those present and the official public purpose of the meeting.

Continuity of reimbursements (dates and/or numerical sequencing of checks issued).

All reimbursed documents are marked "Paid" to preclude their reuse. Determine whether any disbursement transactions are stale dated.

The fund is reimbursed timely (i.e.; monthly) and at year-end.

The authorized fund level is appropriate (i.e.; 2.5 times the monthly expenditure level).

Travel Vouchers.

Travel vouchers can be high-risk transactions because of the possibility of employee manipulations. Fraudulent transactions are usually processed by one employee and are not a systemic problem for the entity. Since Department managers and other supervisors routinely review the travel vouchers for staff members, the highest risk employees who would be able to prepare and process a fraudulent travel vouchers are key managers, department heads, elected public officials, and employees in the accounts payable function. Therefore, concentrate periodic review efforts on higher levels of management officials. Concepts that can help:

The **state per diem system** is preferred over an **"actual" expense system**. Actual expenses are more costly to review and audit, with no significant improvement in the quality of supporting documents. There are many opportunities for fictitious supporting documents to be prepared and submitted for review and approval. Sequential receipts are submitted for expenses at various establishments in multiple cities. Employees are encouraged to falsify receipts for expenses to obtain reimbursement for items that are not otherwise authorized. Employees incur unauthorized expenses or purchase gifts and alcoholic beverages in violation of entity policies. Inappropriate supporting documents are filed with the travel voucher. These include copies of documents rather than originals, charge slips rather than actual receipts, etc.

Credit card statements are not a receipt. It's the underlying transaction receipt that is important. Obtain them. Do not pay from statements only.

Meals and lodging provided by others while attending conferences must be excluded/deducted from employee reimbursement requests. A copy of the conference documents should be standard support for any such travel voucher.

Direct billings by hotels and others must be compared to employee travel vouchers to ensure duplicate expenses are not claimed.

Employee travel expenses for more than one organization should be filed on a single travel voucher and provided to each applicable entity. Original receipts should be filed with the host entity. If there is any question about documentation for such travel, contact the other organization to verify that each entity is paying the correct expenses for the travel. When employees file false travel vouchers for this travel, original source documents are filed with one organization while copies of these documents are filed with the second organization to obtain duplicate reimbursement for the same expenses.

Mileage for employee vicinity travel should be reasonable. Falsifications are difficult to detect. But, obvious errors can be detected by comparing the individual's time sheet to the travel voucher, and by comparing the individual's

vicinity travel voucher to travel vouchers for other specific events during the same time period. These reviews are often not accomplished because of the timing differences in receipt of these documents by managers and supervisors. Periodically review all documents together for specific high risk employees. Duplications or other irregularities occur, such as vicinity travel while out of town on other official business, vicinity travel while not on duty, and vicinity travel when the employee's telephone records indicate a presence in the individual's primary office (i.e.; travel not likely or probable). Determining the individual's physical "imprint" at the office is critical to understanding what really occurred.

Purchasing.

Collusion between a vendor and an organization employee is very difficult to detect, primarily because the employees openly circumvent the system of internal control.

Since off-book purchasing frauds are found as a result of tips and complaints, the entity must have an internal and external communication process that restricts access to buyers by using a central vendor reception area, and informs vendors of entity policies regarding gifts to employees and conflicts of interest. Determine whether the organization sends letters (initial letter and reminder "holiday" letter) to vendors about its **policy on gifts and other inappropriate acts** between its employees and vendors.

Determine if assets are picked-up directly from vendors or delivered to non-standard delivery destinations, versus delivery to a **central delivery destination**. Exceptions to normal procedures should be reviewed very carefully.

Determine if assets are signed-for as received by an organization employee and signed-for as authorized for payment by an organization employee, the two primary signatures noted on purchasing documents. However, also determine if **the positions of the individuals** involved. Employees **act out of character** by doing something that is not a part of their normal job description when fraud is involved.

Determine if vendor invoices include the narrative **description of the items purchased**, particularly on parts for vehicle and maintenance activities. These documents should not include only the part number for the item received. If so, request the vendor to provide the description of the item on future billings. If you can't get them, find another vendor who will provide this important information. The bottom line question is: "**What are you buying?**".

For credit card purchases, ensure that the original source documents support each line item listed on the monthly statement. Do not pay directly from statements without this support. All credit card fraud involves employees making **personal purchases** for their own use. Abuses have occurred for gasoline credit cards and all other types of purchasing credit cards.

Credit Cards.

Credit card fraud occurs when one employee makes personal purchases in violation of entity policies and procedures. It is not a systemic issue within the organization.

Ensure the entity has policies and procedures for the control, issuance, and use of credit cards. Employees should sign an agreement indicating an understanding of the entity's policies and procedures regarding allowable uses for credit cards. Entity training classes for employees is critical to success.

Maintain a log of all credit cards issued, including the signature of each custodian.

Do not pay bills using only the credit card statement.

Obtain and retain original customer sales receipt documents to indicate what was purchased, who purchased it, and the official business purpose. Receipts should include the detail of what was purchased, not simply the total amount of the charge transaction, and make a determination about whether or not the items purchased are legal or allowable. Use an itemized expense voucher if appropriate. Use original source documents only as support for all purchases rather than copies of credit card charge slips.

For gasoline credit cards, maintain a log sheet for each vehicle to record the date of the transaction, amount of fuel purchases, mileage of the vehicle, and the name of the purchaser. Monitor vehicle usage by comparing gallons of gasoline purchased versus mileage driven over a period of time.

Telephones.

Telephone [i.e.; State Controlled Area Network (SCAN), Sprint-Plus, etc.] fraud occurs when one employee makes personal calls in violation of entity policies and procedures.

There are no records maintained on personal local calls in these systems. Some use is normal and to be expected; but, the use must be reasonable as determined by entity policy. Monitoring is the important issue.

Block access for international calls from all employees except where such use would be normal or expected (i.e.; key executive levels only).

Monitor monthly long-distance telephone bills for employees promptly. Scan statements for unusual activity such as calls before or after normal duty hours and out-of state calls.

Personal long-distance telephone use and cellular telephone use must be monitored. Ensure all employees certify monthly statements that all telephone calls are for official business purposes. Identify abuses promptly, seek reimbursement of all personal expenses, and take appropriate personnel actions as deemed necessary when abuses occur. Entity training classes for employees is critical to success.

Monitor monthly cellular telephone use to ensure that employees are enrolled in the appropriate plan for the amount of time actually being used. Reduce plan minutes

purchased if actual employee use does not justify continuing with the original plan selected. Increase plan minutes purchased if actual employee use consistently exceeds the original plan selected. The objective is to obtain telephone services at the least cost.

Proprietary Fund Operations.

If the organization manages a **proprietary fund** that is essentially a "break-even" type operation, such as an automotive repair facility or other equipment repair facility, make sure that revenues and expenditures are reasonable. Any significant variance should be promptly investigated.

Make sure that **organization policies** cover all proprietary fund operations, and include such things as use of prenumbered work orders, advance deposits for the work to be performed, systems to track purchases to work orders, collection of all fees by an independent party separate from the proprietary fund operation, procedures governing use of the facilities by students and instructors, a system to ensure equal access to the facility by all users, etc.

Take inventories of projects in all proprietary funds on a prescribed frequency and ensure that projects continually flow through the facility. Outdated work order numbers and projects that appear on multiple inventory lists over time are high risk transactions that could involve manipulations of inventories.

CASH DISBURSEMENT FRAUD SCHEMES

The ultimate objective of any cash disbursement scheme is a check issued by the entity which is then converted to cash for personal gain.

EMPLOYEES ISSUE PRENUMBERED CHECKS TO CASH, TO THEIR PERSONAL BUSINESS, OR TO THEMSELVES

The most common type of cash disbursement fraud scheme is a fund custodian who disburses funds from checking accounts by simply issuing prenumbered checks to cash, to their personal business, or to themselves. Perpetrators normally falsify entity accounting records to conceal these unauthorized transactions only when a supervisor reviews the function. An individual working alone makes no attempt to conceal these activities in either the check register or the accounting records. These entities have a high risk for fraud because the system of internal control ranges all the way from weak to non-existent.

Unauthorized disbursements are made from all types of bank checking accounts, including: (a) imprest fund accounts to carry out miscellaneous entity purposes (i.e.; petty cash funds, purchasing funds, and advance travel funds); (b) trust fund accounts where there is a fiduciary responsibility over the funds (i.e.; jail inmate trust funds and court bail pending trust funds); (c) depository accounts where revenue collections are initially deposited before transmittal to a central treasurer function where they are subsequently recorded in the entity's accounting system (i.e.; specific function or entire entity); and,(d) general disbursement accounts to carry out general entity purposes. The amount of funds embezzled varies with the type of account (i.e.; under $5,000 in imprest funds, under $50,000 in trust funds, and up to $1.2 million in general disbursements).

Comparing the check number, payee name, date, and amount on canceled checks to check register entries is the most critical audit step performed during reviews of the supporting documents for disbursement transactions. Not performing this test is the fatal flaw in most audit failures to detect disbursement frauds. But, in the paperless society, banks are not returning canceled checks to customers. Under these circumstances, this audit test must be made by reviewing all canceled checks over a period of time using bank microfilm records rather than by reviewing a sequential block of check numbers on file at the entity.

The authorized fund level for most imprest funds should be about 2.5 times the amount of expenditures normally expected in each reimbursement cycle. Because of their relatively small amount, these transactions are first processed through these funds and then reimbursed through the entity accounts payable system. These funds should be reimbursed routinely, when the fund level is depleted to a specified level, and at the end of the fiscal accounting period.

Employees often manipulated these funds as follows:

Advance Travel Fund. Custodians borrow money from the account by manipulating transactions for themselves. They either issue advances to themselves when no travel has been authorized, or fail to repay advances made to themselves for authorized travel purposes.

Petty Cash Fund. Custodians process fictitious transactions for refunds, credits, voids, and other miscellaneous paid-outs.

Purchasing Fund. Custodians write checks to cash, to their personal business, or to themselves. There are no supporting documents for these fraudulent transactions, and canceled or redeemed checks are destroyed. In other disbursement schemes, supporting documents are falsified, altered, or represent xerox copies of vendor invoices which have been previously processed through the entity's accounts payable system for payment. Documents from legitimate expenditures are also used more than once for reimbursement purposes (i.e.; duplicate payments due to failure to mark these documents "paid" to preclude their reuse).

Internal control procedures for checking accounts.

The "front door". This is the authorization and approval process. For imprest, trust, and depository checking accounts, there usually is no authorization and approval process. But, when this procedure exists for general disbursement accounts, all fraud occurs after approval. Perpetrators misappropriate funds by:

Circumventing the authorization and approval process. Methods used to neutralize this procedure include: (a) having the approval authority pre-sign blank checks; (b) using a facsimile signature stamp or plate for the second check signature; (c) using blank (unnumbered) checks for unauthorized disbursements or to replace legitimate checks previously approved; and, (d) preparing two checks for the same disbursement (using either prenumbered or blank checks), having different approval authorities sign them, mailing one of the checks to the legitimate vendor, and altering the remaining check for personal gain.

Altering checks after approval (forgery). Methods used to change the check payee name include: (a) using white-out; (b) modifying the name (i.e.; UPS changed to UPSampson); and, (c) adding the individuals name above the payee line.

Falsifying check registers. Methods used to conceal these activities include: (a) indicating that the check has been issued to other than themselves (i.e.; a legitimate vendor); or, (b) indicating that the check has been voided.

Destroying the integrity of the redeemed check file. Methods used to accomplish this include: (a) destroying redeemed checks (i.e.; missing in

sequence); or, (b) replacing redeemed blank checks with original or xerox copies of uncancelled, prenumbered checks (created prior to any falsification action).

The "back door". This is someone independent of the fund custodian who either reviews the monthly bank reconciliation that the custodian prepares, or actually performs the bank reconciliation themselves. The monthly bank statement must be delivered to this disinterested party unopened, and the review must be accomplished with copies of all canceled and voided checks present. This is the most critical procedure used to deter disbursement frauds because detection of any manipulation is certain.

Red Flags:

No management review or oversight of the disbursement function.

Inappropriate employee segregation of duties.

There is no authorization and approval process for check disbursements.

When two signatures are required for disbursements, blank checks in the checkbook are signed in advance by one of the authorized signatories on the account.

Inappropriate access to the facsimile signature stamp or plate used for the second signatory on an account.

Monthly bank account reconciliation is not performed in a timely manner.

Monthly bank account reconciliation is not performed (preferably) or reviewed by an independent party who is independent of the custodian and who is trained to identify transaction attributes which might be fraud.

Inappropriate storage and issue controls over check stock.

Blank (unnumbered) checks are used (high risk documents).

Check registers are not mathematically accurate.

Check registers or supporting documents appear to be falsified or altered.

Check number, payee name, date, or amount on canceled checks does not agree with entries in the check register.

Voided checks are not retained on file (i.e.; destroyed).

Uncancelled or xerox prenumbered checks are in the file (i.e.; substitution of blank checks for prenumbered checks).

While the check register indicates that checks have been voided, these checks appear on subsequent bank statements (i.e.; redeemed and clear the bank).

Supporting documents and canceled or redeemed checks are not available for certain disbursement transactions (destroyed).

Vendor invoices are not original source documents (i.e.; xerox copies).

Check endorsements are made payable to a third party (i.e.; collusion).

Bank or other financial institution names are the payee on checks (i.e.; to obtain money orders or cashiers checks).

Checks are issued to individuals for large, even dollar amounts.

Check endorsements by local banks for out-of-town vendors (i.e.; fictitious vendor or unauthorized check conversion for a legitimate vendor).

Abbreviated payee names (i.e.; IBM and UPS) are used on checks (high risk due to easy alteration).

Any other unusual check attribute determined by intuition, inquisitiveness, and experience.

Imprest fund balances are excessive.

Advance travel fund advances are made to individuals who performed no travel or are not supported by appropriate approval documents.

Advance travel fund advances are not repaid promptly (i.e.; within 10 days after completion of travel).

Multiple travel advances are outstanding to the same individual.

Funds advanced to individuals from petty cash and purchasing imprest funds are not documented (i.e.; check number, name, date, purpose, amount, and signature).

Petty cash and purchasing documents are not prenumbered and controlled.

Petty cash fund refunds, credits, voids, and other miscellaneous paid-outs are not properly supported by authorizing documents.

Disbursement documents are not marked “paid” after reimbursement to preclude their reuse.

Stale-dated supporting documents (i.e.; dated after last fund reimbursement) are present in the imprest fund.

Purchasing or petty cash forms are returned to the preparer (source) after approval rather then sent directly to the fund custodian for payment.

Fraud Detection:

Schedule all checking accounts for audit on a cyclical basis, know the most common fraud schemes used to misappropriate funds from checking accounts, be aware of red flags for redeemed checks, and understand the critical internal control procedures associated with checking accounts.

Review the checkbook for pre-signed checks during unannounced cash counts.

Review expenditure supporting documents for propriety and for original vendor invoices.

Compare redeemed checks to the bank statement and to entries in the check register.

Prove the mathematical accuracy of check registers.

Review all disbursement documents for imprest fund reimbursements for propriety and for any alterations (forgery).

Perform an unannounced cash count of all imprest funds and agree the amount to the authorized fund level.

Determine whether the fund level is appropriate.

CASE EXAMPLES

A university faculty advisor stole $35,000 from the revenue of a student fund-raising coffee shop operation by writing checks to cash or to himself, by making unauthorized personal loans, and by paying his own personal bills from the account. There was no management review of the depository checking account for this function at any time. While the coffee shop had been created to provide scholarships to art department students, no scholarships had ever been awarded. No one ever questioned why the coffee shop existed. There was no formal agreement with the university, and no payments were ever made for utilities or for the use of the space for the coffee shop facility. The coffee shop was not a part of the university's formal financial accounting system, and financial statements had not been prepared in over 5 years.

The controller stole $1.2 million from a private non-profit association by writing checks to cash or to himself and his personal company. This organization received federal grant funding through a state program (pass-through money). This fraud was not detected by the public accounting firm who performed an annual audit over the seven-year period of

this embezzlement. During the audit prior to detection of the fraud, the public accounting firm stratified all disbursements and selected 11 large dollar transactions for use in their voucher (disbursement) test. The controller was unable to find any supporting documents for 10 of these 11 transactions (all 10 were written to himself). Instead, supporting documents for 10 other transactions of similar size were provided to the auditors by the controller so that this test could be completed. The auditors accepted these transactions from the controller without question. All unauthorized checks were destroyed by the controller when the monthly bank statement was received. He issued an average of $30,000 per month in unauthorized disbursements to himself and his personal company, with the largest single transaction being $50,000. The amount of this fraud equaled 17% of the entity's total revenues, and 20% of it's total expenditures after payroll (i.e.; material to the entity's financial statements). When the press asked about the audit, one of the partners of the public accounting firm was quoted in a newspaper article as follows: "We followed generally accepted accounting standards to the letter. We did a thoroughly professional job on those audits. This is sometimes difficult for the public to understand, but financial audits are not designed to detect fraud or collusion within an organization." These remarks were made after SAS No. 53, "The Auditor's Responsibility to Detect and Report Errors and Irregularities", was issued. A jury acknowledged this audit failure by the public accounting firm and awarded the private non-profit association $1 million in damages. The average citizen understands how this fraud was perpetrated, but can't understand why auditors failed to detect it (the expectation gap). The remaining $200,000 of loss was obtained from restitution by the controller.

The clerk-treasurer stole $8,300 from a small town by using the general disbursement warrant (checking) account for unauthorized purposes. When warrants were issued to cash or to himself, the warrant register was falsified to indicate that these warrants had been voided. When warrants were issued to vendors to purchase assets for his own personal use, the warrant register was falsified to indicate that the transactions were for legitimate vendors. In one instance, the warrant register indicated that the disbursement was made to the Department of Labor and Industries when a dishwasher was purchased from a department store for his girlfriend. In another instance, the warrant register indicated that the disbursement was made to the Employment Security Department when a computer was purchased for himself. While these warrants were redeemed by the bank and appeared on the monthly bank statement, they had been destroyed by the clerk-treasurer. This is a good example of a case where the individual perpetrated more than one type of fraud at the same time. When answering the question: "What else does this person do?", the auditor found that this individual perpetrated an additional $10,100 water utility cash receipts fraud. He made short bank deposits after recording accountability for these funds and marking all customer accounts "paid".

A commercial creamery company bookkeeper stole $503,000 by issuing pre-signed checks to herself over a 3 year period. The bookkeeper was allowed to use pre-signed checks to pay company bills on various occasions. Instead of paying bills, she wrote 21 checks to herself, including one for $52,500. She then used bookkeeping gimmicks to hide the thefts on company ledgers. When this scheme was detected, the company called the individual's prior employer, a home furnishings company, to alert them to the

scheme. This company then detected that the individual had stolen an additional $63,000 from them.

A cemetery bookkeeper stole $330,000 by issuing checks to herself over a 15 year period. Since both partners of the company signed checks to pay bills for the cemetery's operation, the bookkeeper manipulated the partners to perpetrate this scheme. She prepared checks to pay legitimate bills and submitted them to the first partner for signature. She then prepared additional checks to pay the same bills and submitted them to the second partner for signature. While one set of checks were used to pay bills, the bookkeeper altered the payee of the other checks to her own name and cashed them. This individual also performed the monthly bank reconciliation. Thus, no one noticed any of these irregularities.

A mail room supervisor at a public hospital stole $373,000 over 6 years by processing fictitious claims for reimbursement from the imprest fund for stamp expenses. Even though the hospital had a postage meter, the supervisor turned in up to 20 receipts for stamps each day. He purchased stamps at the post office, but asked them for multiple receipts which were reportedly for different accounting divisions (i.e.; a $5 purchase of stamps resulted in 4 receipts for $1.25 each). Each receipt included the official postal service seal, but was subsequently altered by increasing the amount (i.e.; $21.25, $41.25, $81.25, etc.).

An imprest fund custodian of a purchasing cooperative stole $2,600 by writing checks to cash and to herself. The payee line of checks was altered (using white-out) after the documents had been authorized and approved (bank liability). While the initial checks were made payable to legitimate vendors, those payments were processed through the entity's accounts payable system. The supporting documents for the fraudulent imprest fund disbursements were duplicate (xerox) copies of the original documents. Altered checks were endorsed by the custodian, and destroyed when the monthly bank statement was received. The disinterested party bank reconciliation was performed without reviewing the canceled checks (perfunctory). This employee had six aliases, was a drug informant for the police, and was a prior convicted felon (hired a criminal).

The business manager of a small school district stole $2,500 by writing checks to cash and to herself from an advance travel fund and a purchasing fund. There were no supporting documents for these transactions. When the fraud was detected, the auditors asked: "What else does this person do?" Since she was totally responsible for the district's financial operations, additional audit tests of cash receipts and cash disbursements revealed additional losses of $16,500. She used a district credit card to purchase items for personal use, took mid-month payroll draws but did not deduct them from end-of-month payroll, and stole all lunchroom cash receipts from an elementary school which was located next door to the district's offices (these funds had been transmitted to her for bank deposit).

Lake Washington School District - $188,307

Scheme. Largest imprest fund/checking account fraud case. This is a money laundering scheme involving a $15,000 advance travel fund bank account (public funds) and an employee fund bank account (non-public funds). The custodian embezzled these funds during the period May 1992 through February 1997 (five years). Miscellaneous revenue checks from the General Fund were stolen from a variety of sources, including: telephone and soft drink companies, student fees, facility rent for athletic fields and buildings, Parent Teacher Student Association donations, reimbursements for food service and print shop activities, recycling fees, and other individuals, businesses and governments. Since no district function expected these funds, and since district expenses were not directly associated with these revenue sources, there were no consequences associated with the theft and no one missed the money.

The custodian stole miscellaneous revenue checks and deposited them into an employee fund ($133,325). She then issued checks to herself, deposited them into a personal bank account, and used the funds for personal benefit. She also issued checks to various credit card companies and to many businesses and individuals to pay for other personal expenses.

The advance travel fund scheme ($54,982) had three components.

(a) The custodian issued checks made payable to herself and deposited them into her personal bank account. Some checks were also issued to pay her credit card accounts and a development company. None of these 80 disbursements were for authorized travel purposes, and there were no supporting documents for these fictitious transactions.

(b) The payee on these checks was altered by the custodian after they were returned with the monthly bank statement by erasing her name from the payee line and replacing it with the names of other district employees. She then concealed this action by using a rubber stamp to imprint the word “Received” over the alteration. The advance travel fund always reconciled and agreed with the authorized fund amount.

(c) Unrecorded miscellaneous revenue checks were stolen and deposited into the advance travel fund to offset the initial advance transaction. This action transferred the loss to miscellaneous revenue accounts in the General Fund.

Detection. This fraud was detected during a routine audit when an assistant state auditor reviewed endorsements on canceled checks from the fund. While the payee on checks listed the names of various district employees, the checks were endorsed by the custodian and deposited into her personal bank account. The employee was confronted and confessed by stating that she had only manipulated transactions in the advance travel fund and that she had used the money simply to pay bills. However, she did not know how much she had taken or how long the scheme had been operated. The employee’s employment at the district was terminated. During a review of the employee’s personal banking records, additional deposits from a district employee fund were noted. The fraud case was then expanded to include both checking accounts. District policies and procedures were circumvented.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Segregation of duties problem. Custodian prepared checks, used a signature stamp to authorize disbursements, and reconciled the checking account. She also handled miscellaneous revenue transactions processed in an uncontrolled environment. There was no monitoring.

(2) There were no supporting documents for any of the fictitious travel advance transactions, and individuals who authorized travel never saw the actual check disbursement activity. The check signature stamp was not adequately controlled to preclude abuse.

(3) The bank account was not reconciled by a disinterested party by trained personnel who receive the statement unopened from the bank. Checks were not properly voided.

(4) The district did not adequately control checks which arrived through the mail.

Detection Steps.

(1) Review the segregation of duties for bank account custodians with an emphasis on the disinterested party bank reconciliation process.

(2) Test advance travel fund transactions to ensure all are properly authorized/supported.

(3) Review check endorsements for irregularities and identify instances where the custodian's name is shown (the detection method in this case). Review check voiding procedures.

(4) Perform analytical review procedures for miscellaneous revenue streams.

(5) Review the entity's procedures for controlling checks which arrive through the mail. Ideally, two people should open the mail, make a list of the transactions, and reconcile revenue totals to subsequent bank deposits (bank-validated deposit slips).

Additional Recommendation To The District.

The district was advised to correct the weaknesses noted above in **every** public and non-public checking account, not just the advance travel fund.

Sentencing: I hesitate to even list the sentencing in this case because it represents one of the lightest sentences a fraud perpetrator ever received for a significant fraud case in government in the State of Washington. It's an exception to the manner in which most cases are handled. But, all judges are different, and there are always extenuating circumstances involved in the individual's life that are considered in determining the length of the sentence. Even though this crime occurred in our largest County, the former employee was sentenced to only one day in jail. The individual also was required to receive 24 months of community supervision as well as some mental health counseling.

Seattle School District (SPICE Program) - $180,913

Scheme.

The district contracts with the City of Seattle to administer the School Programs Involving Community Elders (SPICE) Program which serves meals to and provides activities and employment opportunities for senior citizens.

Largest "off-book" checking account fraud case. For over five years (1990-95), the SPICE Program bookkeeper issued checks made payable to herself ($171,860) and to "cash" ($9,053) from six program bank accounts she controlled (unauthorized disbursements). She cashed these checks or deposited them into her own personal bank account. In determining the amount of loss in this case, we included only those checks which were issued in even dollar amounts of $500 or more (reasonable and conservative). She also forged the Executive Director's signature on a bank signature card. Almost all program accounting records were destroyed prematurely. In addition, the district over billed the city as much as $300,000 for meals provided under a federal grant for over six years (negotiated settlement resulting in additional program losses). The district has a $500,000 personnel dishonesty bond with a $2,500 deductible provision.

Detection. The Executive Director noted bank account irregularities and discussed them with the bookkeeper by phone (absent from the workplace). This included three checks made payable to the bookkeeper ($4,700) and a forged bank signature card for one bank account. The bookkeeper claimed these checks were to repay her for prior transactions where she had deposited her own money into the program bank account to cover funding shortages. This did occur; but, it was not the correct explanation for these fraudulent transactions. We deducted her deposits totaling $4,235 from the amount of loss in this case.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Segregation of duties problem, and abuse of her position as a key, trusted employee of the district. The bookkeeper was responsible for all functions of the SPICE Program, including the bank account. Her work was not appropriately supervised or monitored.

(2) The bank reconciliation was not performed by someone independent of the custodian who received bank statements directly from the bank. In addition, the Executive Director did not know the bank account was maintained "off-book" and outside the district's control. These financial activities of the program were not included in the district's financial statements.

(3) Program accounting records were prematurely destroyed. Thus, no one was able to determine whether further losses actually occurred.

(4) Disbursements from program bank accounts were not appropriately authorized prior to payment. Thus, unauthorized disbursements to the bookkeeper and to "cash" were not noted or investigated by district officials.

Detection Steps.

(1) Ensure all bank accounts are included in the district's financial records. By subpoena, perform a "sweep" of all banks to identify accounts held in the name of the district. Compare results to known universe of entity bank accounts from prior audits. These bank accounts had the name of the SPICE Program in the title and would have been detected by using this test.

(2) Review internal controls to ensure proper separation of duties. No one person should control all aspects of an entity checking account. Ensure the bank reconciliation is performed by someone independent of the custodian who receives bank statements directly from the bank. Review check payees and endorsements for irregularities such as for checks issued to the name of the custodian and to "cash". Money laundering activities and unauthorized disbursement transactions are the risk.

(3) Perform analytical review procedures for program revenue streams. An understanding of program revenue sources such as meal sales, fund raising campaigns, and voluntary contributions by meal recipients would be essential in determining that these financial activities were missing from the district's financial statements.

Sentencing: The former employee was sentenced to 50 months in the state penitentiary for this crime.

Department of Fish and Wildlife ($137,467)

Elements of the Fraud.

(1) An Accounts Payable Manager had authority to write warrants, pick-up warrants, and reviewed for warrants issued.

(2) He created warrants made payable to himself, or to pay his own personal bills. He utilized an overstated payable balance and "pseudo vendor numbers".

(3) The employee destroyed warrant registers that included warrants made payable to himself or to pay his own personal bills.

(4) He typically volunteered to pick-up warrants, specifically on the days when he was going to receive the inappropriate warrants.

Red Flags.

(1) Lack of segregation of duties. Employee had input and output authority. He was also responsible for monitoring the activity.

(2) Management oversight over the disbursement process was limited.

(3) Many missing documents. All warrant registers with inappropriate payments were destroyed.

(4) Computer system internal controls were circumvented or not utilized. Employee had authority to override important controls.

Detection Techniques.

(1) Scan canceled checks or warrants.

(2) Compare bank account to canceled checks looking for voids or "missing" checks that clear the bank.

(3) Scanning warrant registers may also be appropriate, but make sure to account for all the warrant registers.

(4) Review purchases and expenditures made by the entity through the use of CAATS. For example: (a) Expenditures by payee; (b) Expenditures by type; or, (c) Expenditures by General Ledger code (revenue, payables, etc.).

(5) Test individual transactions determined to be risky. Look for expenditures that are not properly supported or are inappropriate.

Sentencing: The former employee was sentenced to 3 months in jail for this crime.

EMPLOYEES ISSUE BLANK CHECKS TO THEMSELVES

A common cash disbursement fraud scheme in the accounts payable or claims processing function is an employee who issues blank (unnumbered) checks to themselves. While both prenumbered and blank checks are used in disbursement frauds, blank checks are used most often (i.e.; high risk). Perpetrators falsify entity accounting records to conceal these unauthorized transactions.

The perpetrator is usually a supervisor who has complete control over the cash disbursement function (i.e.; prepares vouchers and check registers, prepares checks for issue, redeems checks from the bank, performs the monthly bank account reconciliation, and files canceled checks). This individual falsifies the check register either as it is prepared (i.e.; employee), or after other employees have initially prepared it accurately (i.e.; supervisor).

Since the totals from the check register are used to make the entries in the accounting system, the balance of cash in the bank account is always correct because checks (both prenumbered and blank) clear the bank in the amount recorded as total disbursements.

All unauthorized blank checks are endorsed by the employee, clear the bank, are redeemed by the entity, and are destroyed by the perpetrator to conceal the loss.

There are two ways to falsify the check register:

> Fraud Number 1. Individual transactions on the check register are falsified. All data entries for altered transactions are accurate, except for the amount which has been increased to agree with the amount of funds stolen. When prenumbered checks are used for normal disbursements, a blank check is issued in the name of the perpetrator in an amount which corresponds to the total of the increased amounts. The total of all individual entries equals the total of all disbursements listed on the document (i.e.; mathematically accurate). The supporting documents (i.e.; canceled checks and claims voucher documents) for the altered transactions do not agree with the check register entries. An example of this scheme follows:

Accounting Record	Date	Check Number	Vendor/ Payee	Amount
Check Register	May 10, 1999	11111	Jones Co.	$1,000
Prenumbered Check	May 10, 1999	11111	Jones Co.	$ 500
Vendor Invoice	Apr 30, 1999	-------	Jones Co.	$ 500
Blank Check Not Shown on Check Register	May 10, 1999	XXXX	Treasurer	$ 500

Fraud Number 2. Check register totals are falsified. All data entries for each transaction on the check register are accurate. Only the total amount listed for all disbursements is increased to agree with the amount of funds stolen (i.e.; plugged). When prenumbered checks are used for normal disbursements, a blank check is issued in the name of the perpetrator in an amount which corresponds to the increased amount. The total of all individual entries does not equal the total of all disbursements listed on the document (i.e.; mathematically inaccurate). An example of this scheme follows:

Check Register	Date	Amount	Payee
Total Amount Shown	May 10, 1999	$10,000	-------
Actual Total Amount	May 10, 1999	$ 9,000	-------
Blank Check Not Shown on Check Register	May 10, 1991	$ 1,000	Treasurer

Red Flags:

No management review or oversight of the disbursement function.

Inappropriate employee segregation of duties.

There is no authorization and approval process for check disbursements.

Monthly bank account reconciliation is not performed in a timely manner, or is not reviewed by an independent party.

Inappropriate storage and issue controls over check stock.

Use of blank (unnumbered) checks.

Check registers are not mathematically accurate.

Check registers or supporting documents appear to be falsified or altered.

Check number, payee name, date, or amount on canceled checks does not agree with entries in the check register.

Blank (unnumbered) checks are used for disbursement purposes.

Fraud Detection:

Review expenditure supporting documents for propriety and for original vendor invoices.

Compare redeemed checks to the bank statement and to entries in the check register.

Prove the mathematical accuracy of check registers.

Review all disbursement documents for alterations (forgery).

CASE EXAMPLE

A city clerk-treasurer stole $45,800 over a four year period in the accounts payable function. This supervisor had complete control over cash disbursements, and altered check registers after these documents had been accurately prepared by other employees. She later claimed these documents were corrected because her subordinates made a lot of mistakes (human error). The clerk-treasurer falsified both individual transaction amounts and the total amount on the city's check registers. She then issued blank checks to herself in a corresponding amount that was similar to a normal payroll transaction (about $800 each). She purposefully did this in the unlikely event that the city manager would ever question these transactions. Blindly trusting this employee, the city manager signed all documents the clerk-treasurer brought to him, including all the blank checks for all the fraudulent transactions. He apparently signed checks the same way many people sign routine correspondence, and lost his job for performing this perfunctory review function. These checks were endorsed and redeemed by the city. After the bank statement was mailed to the clerk-treasurer, she performed the monthly bank account reconciliation and destroyed all fraudulent checks. There were no supporting documents for these unauthorized transactions. This fraud was not detected during the first audit because the auditors accepted the first plausible explanation the clerk-treasurer gave them for errors contained in their expenditure tests (human error). When a persistent auditor subsequently detected the fraud, she removed falsified documents from the entity as they were found (protection). After being questioned about these irregularities, the clerk-treasurer failed in an attempt to have the auditor removed from the job (claimed employee harassment). She then moved all current year records to the attic and torched city hall. After confessing to the embezzlement, this 13 year employee immediately paid

the city for the amount of the loss plus audit costs (greed). Her husband was a wealthy contractor.

Public Utility District No. 2 of Grant County ($236,925)

Scheme. Deputy Treasurer/Controller processed 3 fictitious disbursement transactions using legitimate vendors (1 year). These warrants were returned to the employee for hand-delivery. He used improperly voided warrants from printer set-up to issue warrants to himself. An optical scanner/computer printer/color copier was used to forge the signature on the warrants to himself and affix false organization and bank proof endorsements on the reverse side of the fictitious warrants. He altered the warrant redemption computer program to change his personal warrant information to the information from the original fictitious transactions. He intercepted/changed the warrant redemption exception report and substituted the warrants in the PUD's files. Some documents were also destroyed.

Detection. Before he could access warrants being redeemed, his assistant found a warrant issued to the employee and confronted him. All 3 transactions used the same warrant number, and this element was shown on the exception report. If different warrant numbers had been used, this scheme would not have been detected (yet).

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) Data processing functions were performed in the accounting department (no documentation).

(2) Segregation of duties problem. Input (prepare/authorize disbursements) and output (obtain warrants) functions were performed by the same person, a common practice at the PUD.

(3) Redeemed warrants were not distributed unopened to a disinterested party (the warrant redemption clerk) for processing - same procedures for all bank accounts. Warrant list not scanned for irregularities ("ringers") in numerical sequence.

(4) Warrants were improperly voided/inadequately controlled. Warrant issuance log in pencil.

Detection Steps. Determine if:

(1) All computer programming is performed by the data processing function and documented.

(2) The warrant redemption function is properly performed independent of the disbursement function by properly trained personnel using warrants delivered unopened from the bank. Duplicate warrant number edits should exist and be disclosed on exception reports.

(3) Anyone preparing/authorizing disbursements also receives the warrants (input/output segregation of duties review).

(4) Warrant stock and voided warrants are properly safeguarded, and manual warrants are properly authorized, recorded, and supported. Properly follow-up on missing documents.

(5) IRS arbitrage payments are accurate (recompute and verify to supporting documents).

Sentencing. The ex-Deputy Treasurer/Controller was prosecuted by the U.S. Department of Justice, United States Attorney, in United States District Court, Eastern District of Washington. Charged with counterfeiting and money laundering, he was sentenced to imprisonment in the United States Bureau of Prisons for a term of 15 months. Upon release from imprisonment, he will be on supervised release for a term of three years and must complete 150 hours of community service as directed by Probation. The ex-Deputy Treasurer/Controller made full restitution to the PUD for the amount of loss, plus interest, and audit costs prior to entering a guilty plea in the case (no trial).

EMPLOYEES ISSUE PRENUMBERED CHECKS TO FICTITIOUS COMPANIES

Another common cash disbursement fraud scheme in the accounts payable or claims processing function is an employee who issues prenumbered checks to fictitious companies. Since these trusted employees are usually the only employee in the cash disbursement function, or the only employee in the entity, they're able to operate in secret without being detected by managers. Perpetrators falsify individual disbursement transactions after disbursements have been approved by the governing body to conceal these unauthorized transactions. If there is an authorization and approval process, all fraud occurs after that point. A check register is then prepared to agree with the total of all checks issued (i.e.; both legitimate and fictitious checks). All unauthorized prenumbered checks are endorsed by the employee, clear the bank, and are redeemed by the entity. These checks are also destroyed by the perpetrator to conceal the loss (if possible).

Red Flags:

No management review or oversight of the disbursement function.

Inappropriate employee segregation of duties.

There is no authorization and approval process for check disbursements.

Monthly bank account reconciliation is not performed in a timely manner, or is not reviewed by a disinterested party.

Inappropriate storage and issue controls over blank check stock.

Total entity disbursements appear to be excessive, with no reasonable explanation, or the entity has gone into debt to obtain capital to meet normal operating requirements.

The entity does not have a budget, or does not monitor the progress of actual to budget expenses when a budget has been prepared.

Check registers or supporting documents are prepared in pencil, or appear to be falsified or altered.

Supporting documents and canceled or redeemed checks are not available for certain disbursement transactions (destroyed).

Vendor invoices are not original source documents (i.e.; xerox copies) or are stale-dated (i.e.; repetitive use).

An address change in an account is immediately followed by a payment.

Vendor invoices indicate no street address (i.e.; post office box address only).

Vendors are not listed in the telephone book.

Check endorsements for multiple vendors have unexplained similarities.

Any other unusual check attribute determined by intuition, inquisitiveness, and experience.

Fraud Detection:

Review expenditure supporting documents for propriety and for current or original vendor invoices.

Compare redeemed checks to the bank statement and to entries in the check register.

Review check endorsements carefully.

Prove the mathematical accuracy of check registers.

Review all disbursement documents for alterations (forgery).

Review entity budget preparation and monitoring procedures.

Perform a comparative analysis of all expenditures to determine unexplained variances from prior years.

CASE EXAMPLE

A secretary in an irrigation district stole $191,700 over a nine year period in a cash disbursement scheme by issuing prenumbered checks to 20 fictitious companies. She embezzled an additional $54,300 in cash receipts. There was no system of internal control because one person acted with absolutely no management review or oversight in the cash receipt and cash disbursement functions. She was the only employee (part-time) of a small entity which didn't even have an office (committed this crime from the comfort of her kitchen). Vouchers were initially prepared correctly by the secretary and submitted to the governing body for approval. These included incomplete documents, documents without totals, and documents completed in pencil. These documents were, in effect, blank checks. All documents were altered after approval. She used white-out to make changes to these documents at first, but later prepared the vouchers in pencil to make it easier to alter them. Claims vouchers were altered by changing the vendor names, addresses, and amounts, and by preparing false (but believable) supporting documents to agree with the revised claims vouchers. After all unauthorized changes had been made, she issued prenumbered checks for all disbursement transactions. These documents were sent to the county auditor, who signed them and returned them to the district for mailing. The secretary then endorsed the checks and deposited them into a single personal bank account (her own). Check registers, vouchers, supporting documents, and redeemed checks were filed at the county. This fraud was not detected during routine audits, and fictitious documents were included in the auditor's voucher tests. When district expenditures exceeded revenues, auditors recommended the district raise water rates to recover their costs (not supposed to be a non-profit corporation). This caused a taxpayer revolt. When the fraud was detected, the district had $130,000 in outstanding registered warrants (debt), all of which had been stolen by the district secretary. The district did not record the amount of expenditures they approved in their minutes, and they did not ask for nor receive any accounting reports from the county on financial operations. None of the three members of the governing body were removed from public office for non-feasance, but two resigned.

CASEWORKERS WHO PROCESS FICTITIOUS (OR DUPLICATE) AUTHORIZATIONS FOR SERVICE IN PUBLIC BENEFIT PROGRAMS

Another common cash disbursement fraud scheme involves employees who manipulate input transactions for authorizations for service in public benefit programs. These fictitious or duplicate transactions cause computer systems to produce check payments which are then misappropriated. Perpetrators falsify entity accounting records to conceal these unauthorized transactions.

> Payments in fictitious files. Caseworkers perpetrate most public benefit program fraud schemes in short duration case files (high risk) which are subsequently closed or revert to inactive status. In the period of time between routine supervisory reviews of their active case files (20% of cases), caseworkers create fictitious claimant files, process transactions for a short period of time, and then close them to avoid detection.

Fictitious payments in legitimate files. Caseworkers process fictitious transactions in legitimate case files which have been scheduled for closure by using "data diddling" to manipulate computer records in order to receive unauthorized payments from all types of disbursement systems (i.e.; public benefit programs, payroll systems, and retirement systems). The date of death or other termination date is a critical element is determining when a legitimate entitlement to a continuing benefit has ceased. When a trustee reports that a recipient has died, or the period of entitlement to a temporary benefit has lapsed, caseworkers modify the computer file to allow fraudulent transactions to be processed. They access the computer file, change the address of the deceased person to a post office box or other address under their control, and then allow one or more payments to be processed (fraudulent). After the disbursement cycle has been completed, they access the computer file again, change the address of the deceased person back to it's original condition, and declare them dead. This change in the record is called "data diddling". Trustees (outsiders) perpetrate this same crime by failing to report the death of program recipients.

Duplicate payments in legitimate files. Caseworkers process duplicate (fictitious) transactions in legitimate case files to manipulate computer records to receive unauthorized payments from disbursement systems in public benefit programs.

Inspector General of the U.S. Department of Health and Human Services Report. These fraud schemes were confirmed in a 1983 report entitled "Computer-Related Fraud And Abuse In Government Agencies". The report stated that fraud perpetrators were non-supervisory employees who primarily were authorized functional users of the computer system rather than data processing personnel. Half of all cases were detected by accident, with confirmed losses ranging up to $177,400 per case (actual losses thought to be higher). The most common job type was that of a caseworker who determined eligibility and amount of payments to be made to program beneficiaries, and who created input documents away from the computer. These documents were later entered into the system by another person. Perpetrators either created unauthorized files or records, or manipulated existing files or records. Half of these individuals destroyed the documents evidencing the crime, and 75% had co-conspirators (mostly people outside the agency). The median frequency for committing the criminal act was only 8 times, and the median duration of the crimes was 6 months. Most perpetrators were disgruntled employees seeking revenge on their organization or immediate supervisor (i.e.; lack of promotion, low pay, etc.). Computer security and system controls were weak. Employee crime was a low priority for managers, who had no knowledge of the systems. Perpetrators suggested the following ways to strengthen these computer systems: (a) random case validation; (b) rotate case load; (c) identify workers with their transactions in the data base; (d) limit access within the system; and, (e) enforce security features.

Red Flags:

Supervisory reviews of caseworker files are not performed, or are scheduled events which involve only active case files.

Short duration and closed case files are not routinely reviewed by supervisors.

Payments on continuous cases are made after the date of death (certificate) or after the period of entitlement has lapsed.

Supporting documents appear to be falsified or altered, or original source documents are not in file (i.e.; xerox copies).

Inappropriate employee segregation of duties.

Inappropriate access to the computer facility or to operator passwords (i.e.; unrestricted access or too many people).

Computer system whose operator passwords do not identify the user with transactions they process in the data base.

Computer system which does not prepare reports identifying any unusual, exception, or special authorization transactions for review and approval by supervisors during routine processing at the end of the business day.

All computer files needed for transaction processing are not linked or accessed. Caseworkers are responsible for too many processing functions (i.e.; preparing authorization for service forms, making computer input for transactions, verifying computer input transactions to computer output reports, and filing authorization for service forms).

Computer edit controls for program limits are not present in the system, or are not present at the proper level of processing to detect irregular transactions either on a reject basis or an exception notice basis.

The entity does not have someone independent of the caseworker function make distribution of authorization for service forms.

The entity does not monitor the use of prenumbered authorization for service forms (i.e.; issuing blank forms to various functions, and reviewing the sequential use thereof after completion).

Office personnel have not been adequately trained to use and review computer output documents and reports.

The entity does not have procedures to monitor employee outside employment and ensure that prohibited relationships are not established.

An address change in an account is immediately followed by a payment.

Fraud Detection:

Use computer assisted audit techniques (CAAT's) to inquiry computer data bases for disbursement systems of all types: (a) to determine whether certain conditions exist (i.e.; fraudulent conditions, such as a charges for a "pregnant man" in a health benefits scheme); or, (b) to acquire data on certain types of transactions for use in further substantive audit testing (i.e.; a list of the universe of a certain type of item to be used as the basis for subsequent audit sampling).

Review the segregation of duties of key employees.

Review the computer operator password access system for propriety.

Review critical computer exception transactions to ensure that all items are valid, properly supported, and approved.

Determine whether any individual limits (i.e.; hours, dollars, etc.) have been exceeded in public benefit programs.

CASE EXAMPLE

A part-time caseworker in a regional public benefit program office stole $177,200 by processing 421 fictitious authorization for service transactions over a two year period. A computer payment system was used to process these fictitious transactions. Because this caseworker used the names of real people who were already receiving services from this program, every transaction processed also represented a duplicate benefit for that individual. In addition, the dollar limit for each person receiving benefits under this program was exceeded each month. This condition was not detected because the computer edit was located only at the data entry terminal. Since this edit was not present at system level, multiple transactions could be processed against the same individual to exceed the dollar limit of this program without detection. All payments went to the caseworker's private consulting business, even though this business did not have a contract with the department. Because of his duties, the caseworker was able to assign a vendor number to his business so that all transactions could be processed. While the payment system computer should have been linked to the computer vendor file and the computer contract file to properly process transactions, it was only linked with the computer vendor file. Thus, while the caseworker's business did not have a contract to provide services to the department, invalid transactions were still able to be processed through the computer payment system without detection. The caseworker used transaction types which resulted in no feedback documents in the system. In addition, the caseworker was responsible for distributing the copies of all authorization for benefit documents, including the copy which went to the program recipient. If these documents had ever been sent to the client (none were), this fraud scheme would have been detected easily by subsequent investigations of customer feedback which said: "I never received this service." During this fraud scheme, the caseworker was transferred to another department where he was not authorized to process transactions in this program. After conducting research in office files, he located the names of additional program recipients and used the computer passwords of other office employees who were authorized to

process these transactions to continue this scheme for another year without detection. While field office personnel were properly trained on how to operate the computer system, they were not adequately trained on how to properly review computer output reports. A program manager detected these fictitious payments by accident when she discovered that the consulting business being paid did not even have a contract to do business with the department.

COMPUTER-RELATED FRAUD IN GOVERNMENT AGENCIES: PERPETRATOR INTERVIEWS

Inspector General of the U.S. Department of Health and Human Services Report. Many fraud schemes were confirmed in a 1983 report entitled "Computer-Related Fraud And Abuse In Government Agencies". Results of June 1983 report:

(l) Fraud cases primarily involved theft of cash or diversion of assets, usually through input manipulation in benefit or payroll systems. Most abuse cases involved use of computer time for outside business or entertainment.

(2) Most perpetrators were Federal, non-supervisory employees. Four out of five of the fraud perpetrators earned $20,000 per year or less. Two-thirds of the fraud perpetrators were functional users of the computer system, rather than data processing personnel.

(3) Confirmed losses ranged up to $177,383 per case, although actual losses were thought to be higher in many cases.

(4) Operating personnel found over half of the frauds and over two-thirds of the abuses. More importantly, half of the cases were detected by accident, which was twice the incidence of detection by either controls or audits/reviews.

There were 5 objectives of this study.

(l) Who Were The Perpetrators?

Virtually all perpetrators were employees rather than outsiders. None were beneficiaries, clients, or hackers.

All perpetrators were authorized users. It was a necessary part of their job either to query, enter, or modify data in the computer system or to direct the operation of the computer system.

Perpetrators were young, good employees (median age of 30).

Many were "students of the computer system" and were called upon to assist others.

25% received performance awards - some for designing or implementing the computer system they ultimately stole from.

Almost 25% had prior criminal records when hired - under special programs for ex-felons or employment as a condition of their probation.

The opportunity to commit fraud was seized more quickly by those with prior records. 40% with a criminal record committed their fraud within one year of being hired. Median length of employment for ex-offenders was 3 years.

(2) What Jobs Did They Have?

Positions of perpetrators ranged from secretaries to senior program managers and from entry level clerks to highly trained systems analysts.

The most common job type (35%) was a caseworker - people who determined eligibility and amount of payment to be made to program beneficiaries.

Next most common jobs were technicians (28%) and clerical (26%).

All perpetrators needed to modify data in the system or have access to the computer itself.
50% performed their jobs through the creation of input documents away from the computer.

75% worked for benefit programs that issued funds, and were in a position to issue those funds.

(3) How Was The Crime Committed?

85% of the perpetrators caused negotiable financial instruments to be issued (checks).

Cases not involving checks included: (a) Restoration of annual leave; (b) Modification of income tax deductions; (c) Keeping funds returned to the agency; (d) Sale of false identification cards; and (e) Sale of information.

"Data diddling" describes those computer crimes where an employee commits the crime by manipulating data before or during the input process, or during output from the computer system - changing beneficiary name, address, or bank account information; or erasing payment history to issue duplicate payments.

90% of all cases involved data diddling.

Almost all cases involved manipulating input to the data system.

Not all perpetrators had direct access to the computer, nor did they require direct access to the computer system to commit their crimes. 50% of cases involving input manipulation were not committed with "hands on" access to a computer. They created documents that were later entered into the system by another person.

There were 3 predominate fraud schemes. Perpetrators either created unauthorized files or records, or manipulated existing files or records.

(a) Manipulation of data on existing cases in an on-going payment system (44%). Three major areas of opportunity: (l) The beneficiary died or lost eligibility; (2) Duplicate payments were issued to relatives who were valid cases; and (3) Dormant cases were reactivated.

(b) Creation of false claims in a one-time payment system going to self or co-conspirators (26%). This is a typical disbursement fraud scheme applicable to any entity/organization.

(c) Creation of false records and addition to files in an on-going payment system (21%). These were the more difficult to accomplish because of the documentation required to establish eligibility.

For on-going payment systems, it was common for the perpetrator to periodically terminate their illegal cases or claims to prevent detection.

50% of perpetrators destroyed the hardcopy evidence of their crime.
Most relied on virtually nonexistent filing systems or on routine, periodic destruction of hardcopy to cover up their crime.

75% of computer-related fraud cases involved co-conspirators (mostly people outside agency).

50% of cases did not require perpetrators to use an identification number and/or password to get data into the system to commit their crime.

Those requiring identification/password identification to commit the fraud did not have any difficulty obtaining the needed data (easy access).

The median frequency for committing the criminal act was only
8 times, which serves to demonstrate the potential efficiency of using a computer to commit a crime. One perpetrator only made 4 unauthorized entries into a benefit program computer and got over $100,000.

The median duration of the crimes was 6 months.

Losses ranged from none to $350,000. The average loss per case was $45,000.

Although none of the perpetrators admitted to stealing more than had been identified in their case as submitted to the court, some implied during the interview that more was stolen.

(4) Why Was The Crime Committed?

75% of perpetrators were influenced by a specific situational stress (need) when they committed their crime. These included: (a) Specific family problem; (b) Specific debts; and (c) Drug Habit.

Most were disgruntled employees seeking revenge on the organization or immediate supervisor (lack of promotion, low pay, etc.). Since they were unhappy employees, this fact made it easier for them to commit their crime.

Few perpetrators voluntarily stopped the fraud once their need (specific situation stress) was met.

25% committed their crime because an opportunity presented itself rather than because of some driving problem.

For others, boredom or free time was the cause. Perpetrators often sat at a computer terminal and tried to "beat" the system in their idle time until they won the game. The fraud scheme started for real once the game was won.

Perpetrators didn't fear being caught or punished.

50% didn't even think about the consequences of their actions.
Most thought their chances of being caught were minimal.

(5) What Was The Work Environment?

Computer security and system controls were weak.

While access controls, edits, and separation of duties were designed into most computer systems, poor implementation at the user level often undermined their intent.

Perpetrators were influenced because of their perception that the system was vulnerable.

67% were aware of other crimes "like theirs".

50% knew of specific crimes, while others had heard of such crimes.

Employee crime was a low priority for managers.

They were the "trusted employee". And, supervisors were naive about their job at the computer terminal.

One of the largest problems is that managers have no knowledge of the systems. Thus, managers manage, and operators operate.

How would perpetrators strengthen the systems?

Random case validation. Cases weren't verified and no one actually spoke to the beneficiary. Even a simple telephone inquiry would have raised the risk of detection

sufficiently to preclude some of the crimes. Perpetrators terminated frauds when periodic case recertifications were due.

Rotate caseload. Most caseworkers had permanently assigned caseloads.

Identify workers with their transactions in the database. Data was anonymously entered into the system. The system wasn't being watched.

Limit access within the system. Override or force codes were used in the system. Data was deleted or edits bypassed. System users' access needs to be limited to only the codes or types of transactions needed to do their job.

Enforce security features. Computer controls were bypassed to promote office efficiency, or neglected.

RETIREMENT SYSTEM SCHEMES

Another common cash disbursement fraud scheme involves individuals (i.e.; both insiders and outsiders) who manipulate retirement systems to cause computer systems to produce check payments which are then misappropriated. Employees falsify entity accounting records to conceal these unauthorized transactions.

Once a person qualifies to receive retirement benefits and is entered into the payment system, subsequent periodic payments are automatic. Recipients do not submit time sheets in order to support payments like the normal payroll system. As long as the individual is entitled to receive benefits and is still alive, all payments are justified. Fraud schemes occur in at least the following three phases of retirement systems.

> Initiation. Employees establish retirement system files for ineligible or fictitious individuals (i.e.; similar to ghost employees in a payroll system).
>
> Continuation. Employees process duplicate transactions in legitimate case files by using “data diddling” to manipulate computer records to receive unauthorized payments (i.e.; the same as caseworkers in public benefits programs as explained above).
>
> Termination. Several methods are used to manipulate accounts within the retirement system. These include the following:
>
> > Employees process fictitious transactions in legitimate case files by using “data diddling” to manipulate computer records to receive unauthorized payments.
> >
> > Trustees (outsiders) perpetrate this same crime by failing to report the death of program recipients.

Employees also falsify program documents to withdraw funds from dormant accounts of individuals who are vested in the retirement system, but who have not yet reached the normal age for retirement.

Early Distributions. Early withdrawals of funds from the retirement system after an employee qualifies for vesting also represent a risk. Before a withdrawal of funds can be made from a member's retirement account, the member must submit a form requesting this action to the Department of Retirement Systems. Key control elements associated with this transaction are: (1) The member must include the address where they want the warrant to be mailed; (2) The member's signature must be notarized. And, (3) The member's signature must also be verified against the Department's master signature on file for the employee. These elements ensure any disbursement is made to an authorized member at the proper address.

Secondary Distributions. If an employer places additional funds on deposit in the retirement system after the employee has made an early withdrawal of funds, these funds must be considered to be extremely high risk. The primary problem associated with any payment after the initial distribution is that the member probably doesn't know the money is on deposit and due to them. So, if they don't receive the money, and they won't, they'll never miss it or know to complain about the situation until the Internal Revenue Service calls upon them, if that happens at all. Once the member asks for all their money to be sent to them, they're completely happy when the payment is received. Few people would actually know exactly how much they were entitled to at this point in their life anyhow. In addition, the employer doesn't notify the member that additional funds have been deposited with the Department because they are not in the notification loop when it comes to the request for withdrawal of funds from the account in the first place. From an internal control standpoint, nothing practical could help at the employer organization. Only an action by the Department of Retirement Systems would make sense to ensure that these funds on deposit are properly disbursed to their rightful owner. If the Department takes no unilateral action, funds in such accounts eventually wind up in the unclaimed funds accounts of the State of Washington. People simply die without knowing the funds are on deposit for them at the Department. Or, someone steals the funds from the accounts and no one is the wiser.

Thus, these accounts must be treated the same as dormant accounts in financial institutions. In the banking world (i.e.; commercial banks, credit unions, and similar financial institutions), dormant depositor customer accounts are tightly controlled because they are the highest risk accounts for manipulation by an employee inside the organization. For example, funds could be stolen from these accounts without the knowledge of the customer because they do not know about the funds that are on deposit at the financial institution or the bank does not have the current address of the customer and has lost contact with them for a variety of reasons. Thus, any withdrawal from a dormant account must be carefully controlled. Under these circumstances, sending the funds on deposit to the customer at any address should be the subject of intense scrutiny by bank management. In fact, unusual precautions should be taken to ensure the funds are subsequently disbursed to the rightful party. As a result, these accounts are removed from the normal account management processes for these very reasons. And, they are

secured in a central file under the watchful eyes of a key manager, supervisor, or vice-president responsible for managing customer accounts.

Retirement systems must review the procedures used to make address changes to any member's account after the initial distribution has been made. Access to these dormant accounts should be severely limited because of the high risk of manipulation as described above. If normal access to address change files continues after the initial disbursement, an unscrupulous employee determined to steal funds from these accounts would probably do one of two things.

- First, they would create a false disbursement, intercept the warrant output before mailing, and then deposit the warrant in their personal bank account. As soon as this was done, they would use "data diddling" to change the address on the file to an address they are able to control, such as a post office box. Changes to the computer address file usually are not formally recorded on transaction registers and do not normally leave an audit trail for managers or auditors. Then, when the computer automatically prepares the annual Form 1099's, the tax notification is mailed to the perpetrator and destroyed. The post office box would then be closed leaving a stale trail for any Internal Revenue Service investigation about the taxes owed on the withdrawal of funds from the account. Any complaint by the account owner about the non-receipt of funds would be hard to deal with at this late point in time (probably one to two years after the second distribution warrant was issued).

- Second, they would use "data diddling" to change the address on the file to an address they are able to control. Then, they would create a false disbursement and let it be mailed normally. After the Form 1099 was received, the post office box would be closed. Basically, this is the same event handled two different ways. The unscrupulous employee would decide which way to do this based on their access to the accounts and the internal control structure in place at the Department.

Therefore, secondary distributions of funds should be handled exactly the same as initial distributions of funds. Once the Department receives funds for a member after the initial distribution has been made, the key manager assigned to control these high risk accounts should send a letter (perhaps even by registered or certified mailing procedures) to the member notifying them of the availability of funds and verifying the current mailing address. A withdrawal request form should be included with the letter. The Department should ask the member to verify the address and have their signature notarized on the form just like they did for the initial distribution. Once received and processed, the second distribution warrant should be issued.

<u>Red Flags</u>:

Supervisory reviews of new or short duration recipient files are not performed.

Payments on continuous cases are made after the date of death indicated on the certified copy of the death certificate.

Supporting documents appear to be falsified or altered, or original source documents are not in file (i.e.; xerox copies).

Inappropriate employee segregation of duties.

Inappropriate access to the computer facility or to operator passwords (i.e.; unrestricted access or too many people).

Computer system whose operator passwords do not identify the user with transactions they process in the data base.

Computer system which does not prepare reports identifying any unusual, exception, or special authorization transactions for review and approval by supervisors during routine processing at the end of the business day.

All computer files needed for transaction processing are not linked or accessed during routine processing.

Caseworkers are responsible for too many processing functions (i.e.; preparing authorization for service forms, making computer input for transactions, verifying computer input transactions to computer output reports, and filing authorization for service forms).

Computer edit controls for program limits are not present in the system, or are not present at the proper level of processing to detect irregular transactions either on a reject basis or an exception notice basis.

The entity does not have someone independent of the caseworker function make distribution of the authorization for service forms.

The entity does not monitor the use of prenumbered authorization for service forms (i.e.; issuing blank forms to various functions, and reviewing the sequential use thereof after completion).

Office personnel have not been adequately trained to use and review computer output documents and reports.

The entity does not have procedures to monitor employee outside employment and then ensure that prohibited relationships are not subsequently established.

Retirement checks returned as undeliverable by the post office (high risk) are held in the retirement system office and are not dealt with promptly.

Retirement refund checks (high risk) are returned to the retirement system office for distribution.

Applications for withdrawal of funds from individual dormant retirement accounts do not require approval of the department head to verify the validity of the transaction (high risk).

An address change in an account is immediately followed by a request for payment.

Early withdrawals from the Retirement System do not require notarized signatures of the member prior to release of funds.

Funds received from employers after an early withdrawal are not treated the same as "dormant" accounts in financial institutions (i.e.; supervisory control of all transactions in such accounts).

Access and procedures for address changes for secondary distributions of funds are not limited or monitored.

Fraud Detection:

Use computer assisted audit techniques (CAAT'S) to inquiry computer data bases for disbursement systems of all types: (a) to determine whether certain conditions exist (i.e.; fraudulent conditions, such as a charge for a "pregnant man" in a health benefits scheme); or, (b) to acquire data on certain types of transactions for use in further substantive audit testing (i.e.; a list of the universe of a certain type of item to be used as the basis for subsequent audit sampling).

Match dead file names against recipient files to identify invalid active files (i.e.; Social Security Administration or state department of vital statistics).

Review the segregation of duties of key employees.

Verify that recipients over a certain age (i.e.; 85, 90, 95, etc.) are still alive.

Review the computer operator password access system for propriety.

Review critical computer exception transactions to ensure that all items are valid, properly supported, and approved.

Review procedures to ensure that retirement benefit, refund, and withdrawal checks are not returned to the retirement system office for distribution.

Review procedures to ensure that all retirement checks returned as undeliverable by the post office are investigated promptly, and that subsequent payments on such accounts are suspended until a proper address has been determined.

Review procedures to ensure that applications for withdrawal of funds from individual dormant retirement accounts are required to be approved by the department head to verify the validity of these transactions.

Review files for early withdrawals and secondary distributions to ensure that the member's signature authorizing release of the funds was notarized and that funds were disbursed to the member's last known current address. Determine if these accounts are treated the same as "dormant" accounts in financial institutions

Review secondary distribution files to ensure that the member's signature authorizing release of the funds was notarized (i.e.; supervisory control of all transactions in such accounts) and that access and procedures for address changes for secondary distributions of funds are extremely limited or monitored.

CASE EXAMPLES

Trustees of retirement system recipients (i.e.; friends and family members) failed to report the death of the retiree. Since all payments were transmitted to the trustee's bank by electronic funds transfer (EFT), these checks did not even have to be endorsed (automatic). These funds were the trustee's only source of income, and were simply spent.

An apartment manager in the Sacramento, CA rented rooms only to elderly individuals receiving retirement checks. This individual befriended the occupants and became their trustee. In this bizarre case, the apartment manager killed the retirees and buried them in the back yard of the complex. The trustee (outsider) failed to report the deaths of multiple retirees. All payments were transmitted to the trustee's bank by EFT, and were simply spent.

An accounting technician in a city retirement system stole $41,100 in pension funds in a six-month period. He used two methods to do this. First, he forged applications to obtain refunds from individual dormant retirement accounts. When these checks were prepared and delivered to the retirement system office, he forged the endorsement on the checks and deposited them into his personal bank account. Next, he manipulated funds in the retirement account for one member whose checks were returned to the retirement system office as undeliverable by the post office. He forged a letter requesting payment of all funds remaining in the account, and stole all the returned checks related to this account. When the check was prepared and delivered to the retirement system office for the withdrawal of the remaining funds in the account, he forged the endorsement on all the checks and deposited them into his personal bank account. This scheme was detected when one individual received a Form 1099 from the city notifying her that the retirement funds withdrawn from the dormant account were taxable income. She certified that these funds had never been received, and that the signature on the check was a forgery. The accounting technician immediately disappeared as soon as this case became known. After this individual left the retirement system office, one additional forged application for a refund from a dormant retirement account was discovered; however, the check for

this transaction ($5,100) was still on-hand in the office and had not yet been misappropriated.

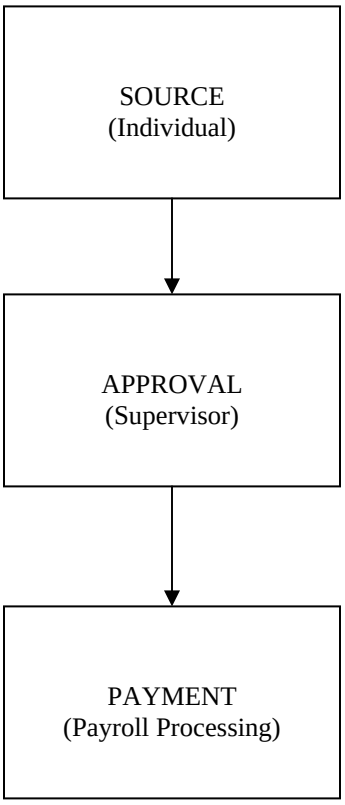
PAYROLL FRAUD SCHEMES

The opportunity for fraud in the payroll function is high when an employee has broad discretionary powers in the work environment, and is not properly supervised. **The audit risk is that an inappropriate or fraudulent payment will be made through the payroll system.**

It's important to know exactly how the payroll system breaks down when it has been compromised. The table below depicts an important concept for managers and auditors. Everyone should always look for a straight line from source to approval to payment.

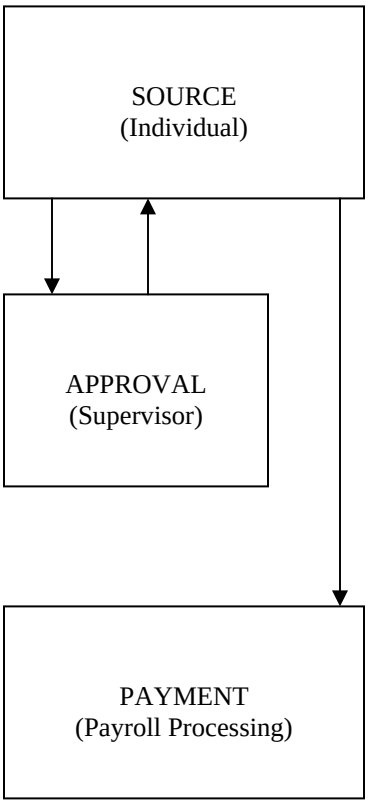
Normal Practice

(The Straight Line Concept)



Irregular Practice

(Fraud)



The Fraud Perpetrator:

- All employees (everyone can do something).

- Department timekeepers (who add unauthorized hours of work).
- Department managers (who sign their own time sheets).
- Payroll Department employee or manager (who add unauthorized hours of work and delete their own leave).

All Employees. Fraud occurs when managers forget that the employee's time sheet is a blank check (i.e.; similar to travel vouchers and petty cash vouchers). Once completed by the employee and approved by the supervisor, this form must be sent directly to the payroll function rather than returned to the employee. All fraud (i.e.; unauthorized work hours or unauthorized overtime hours charged) occurs after approval. The department/function timekeeper is the one person who controls this area and could falsify his/her own time card/sheet/list without detection by an unsuspecting supervisor or other approval authority.

Payroll Department. Employees in the payroll function falsify organization accounting records to conceal unauthorized transactions.

CONCEPTS TO REMEMBER ABOUT PAYROLL

(1) Payroll expenses represent **50-80% of all disbursements in government**. Ensuring that all payroll payments are valid and authorized helps to ensure the public's expectation that funds are spent wisely and for official public purposes. It also assures the public that government is accountable.

(2) **Every** employee in the organization has the opportunity to falsify his/her own time sheet to obtain unauthorized payroll. Thus, internal control procedures in the payroll system must be strong and continually monitored by managers in a decentralized audit environment.

(3) Supervisors should use care when processing documents that serve the same purpose as blank checks. Unauthorized transactions are processed on: (a) petty cash documents; (b) travel vouchers; and (c) **time cards/sheets/lists (payroll). All fraud occurs after approval**. Unused lines on these forms are then completed (falsified/altered/changed/revised). Therefore, eliminate the use of blank lines on these forms (crossed-out). All such documents should proceed directly to payment after approval by a supervisor and not be returned to the employee where they are falsified. **Look for a straight line from source to approval to payment**.

(4) All employee time cards/sheets/lists should be signed or certified by the employee and approved by a supervisor or other designated approval authority for managers at the top of the organization. Systems for electronic time sheets should use

passwords or other access controls to ensure that employees are precluded from accessing supervisory or approval fields. **No one should approve his/her own time sheet**. When an employee works in more than one department/function/unit, one supervisor should be designated to approve the individual's time card/sheet/list. The employee's time worked in another unit should be verified with the supervisor in that unit prior to certification of payroll for payment.

(5) Managers should establish an appropriate **segregation of duties** for all employees throughout the organization, including those individuals involved in payroll processing. No employee should control any transaction from beginning to end.

- For example, key **employees with input and output responsibilities are the "kiss of death"** in disbursement systems (i.e.; accounts payable and payroll functions). These individuals have the ability to process a fictitious transaction and then receive the proceeds of their act (the warrant). Switch duties of each person to eliminate this conflict. When it's not possible to segregate duties between two or more employees, establish a **periodic monitoring program** for this key employee that effectively accomplishes a segregation of duties without hiring another individual to perform the task.

- The Human Resources Department and Payroll Department each have a role to play to ensure that all employees are properly hired, paid their authorized wage while employed, and properly terminated through retirement or by other means at the request of the employee or the organization. Personnel action forms or equivalent documents should be on file in Human Resources to support all changes in employee compensation (i.e.; promotions, pay raises, etc.). These two functions must be specifically segregated to ensure that no one has the ability to establish a ghost employee, change an employee's authorized pay without proper approval, or continue the pay for an employee after termination. Each of these specific acts requires a **manipulation** of payroll records. No one individual should be able to accomplish all actions required to conceal these activities.

(6) There should be an independent review of the payroll distribution list by all Departments. These reports should be routinely distributed and then reviewed and monitored by appropriate managers. This helps to identify ghost employees, bogus overtime, unusual information related to total compensation, and the proper allocation of payroll costs by Department and function.

(7) The COBRA program makes the Payroll Department a **cash receipting function** for these ex-employee payment transactions. Thus, there is a **hidden danger** here because few people realize that money flows through the Payroll Department. In this program, Payroll Department employees: (a) Steal payment checks from ex-employees who pay the organization for their health/medical benefits (i.e.; checks made payable to either the organization or the insurance carrier). (b) Steal warrants the organization issues to the insurance carrier that provides these health/medical benefits for the employees. (c) Alter computer records to extend

an ex-employee's benefit termination date without authorization. And, (d) Provide coverage for health/medical benefits to unauthorized individuals.

Organizations should: (a) Reconcile suspense funds established to process COBRA payments. An agency fund using zero balance accounting procedures may be used for this purpose. (b) Establish computer edits or manual controls to ensure that no one remains in the COBRA program longer than allowed by law. (c) Establish procedures to ensure that all participants are authorized and have been approved for the COBRA program by management. And, (d) Review payment records to ensure that health/medical benefits are continued in force **only** for eligible individuals.

(8) Managers should periodically perform a **ghost employee test** using a payroll list versus making a payroll pay-out. Confirm that employees exist with department employees not performing payroll/leave functions**. Part-time, temporary, seasonal, and terminated employees** are areas of high risk for payroll manipulations. After these individuals leave employment, other employees alter their payroll records in order to receive unauthorized payments on their behalf. In addition, one attribute related to a ghost employee is that the employee does not sign the time card/sheet/list.

(9) Excluding overtime, determine if employees are **paid more than authorized**. Compare gross payroll amounts and income tax withheld to Internal Revenue Service (IRS) Forms W-2 (individual form) and W-3 (organization transmittal to IRS) for agreement. Under-reporting of payroll information to the IRS could be an indicator of fraud.

(10) Ensure **mid-month payroll draws** are authorized, made pursuant to law, and deducted from the employee's end-of-month payroll check. **Only one** interim payroll payment is authorized per month.

(11) Ensure **overtime and stand-by or call-back time** are authorized and properly supported. For stand-by or call-back time, determine if the employee's work unit is authorized to perform this function and maintains appropriate schedules of employees and the dates these categories of work were performed. If this category of work is authorized, determine if the employee occupies an authorized stand-by or call-back time position. If so, determine if the work unit's records indicate that the employee was assigned to work stand-by or call-back time on the dates indicated on their time card/sheet/list. Stratify the population to identify heavy users for subsequent analysis and testing. Overtime for management officials may be unauthorized by organization policy. Testing should include discussions with appropriate supervisors for reasonableness and validity of recorded overtime.

(12) Ensure **sick and annual leave accruals** are in accordance with organization policy and properly input/recorded in the system after approval. Determine if employee annual and sick leave accruals are in excess of **authorized levels**

established by organization policy. Ensure that **maximum year-end balances** are not retained in excess of that authorized unless specifically approved by management. Ensure that sick and annual leave use and "**buy-outs**" are pursuant to organization policy.

(13) Determine if the organization has a policy for **compensatory ("comp") time**. Ensure that all comp time earned is pursuant to organization policy and properly input/recorded in the system after approval. Determine if employees retain comp time in excess of **authorized levels** established by organization policy. Ensure that **maximum year-end balances** are not retained in excess of that authorized unless specifically approved by management. Ensure that comp time use and "**buy-outs**" are pursuant to organization policy. For example, methods of comp time use often vary from organization to organization (i.e.; use at a 1:1 ratio for every hour accrued, or use at a 1.5:1 ratio for every hour accrued).

(14) Review payroll records for the **payroll clerk** or for any other employee who controls the payroll function for all types of payroll transactions, particularly in small entities, because this is the highest risk employee in the organization. The one person who controls this function can falsify his/her own time sheet or change other critical payroll information in the accounting system without detection by an unsuspecting supervisor or approval authority or by a supervisor who does not properly monitor the payroll clerk's actions and activity. The Department or function timekeeper is a mini-payroll clerk in a large organization. Thus, the same situation exists for this employee. For example, someone independent of these critical payroll employees must monitor all activity to ensure that accurate information from time cards/sheets/lists is actually entered into the accounting system and is not subsequently removed.

(15) Compare the amount, payee, and endorsement on redeemed payroll warrants to the actual warrant register for a specified period of time (block sample) for agreement. **Multiple endorsements** on payroll warrants may indicate high risk documents/transactions warranting further review by management. For direct deposit transactions, trace similar information (except for endorsement information) from the direct deposit register (same as warrant register) to the record of funds transferred to the bank.

(16) A **missing or fraudulent** (altered, forged, or fictitious) document is at the heart of every fraud. Accordingly, managers and Payroll Department supervisors should review payroll documents for obvious alterations and be able to readily recognize the authorized signature of individuals who have been designated as certification officials for employee time cards/sheets/lists. These important payroll documents should be retained pursuant to the organization's record retention policy/plan that is filed with and approved by the Archivist of the State of Washington.

(17) The greatest disbursement risk is represented by **manual transactions** that occur between periods represented by computer generated warrant registers. These

manual transactions may be shown as pen and ink changes to computer generated warrant registers, may be omitted entirely (i.e.; gaps in the warrant numbers listed), or may represent duplicate warrants previously processed through the system. Governing bodies may not even approve these transactions if the unauthorized warrants were omitted from the warrant registers.

THE FIVE MOST COMMON PAYROLL FRAUD SCHEMES

(1) **Ghost employees**.

Attributes: (a) Employee never comes to work. (b) Time sheet is not signed by employee. (c) Dual endorsements on payroll warrants.

High risk employees: (a) Part-time, seasonal, or temporary employees. (b) Employees who terminate employment at the organization.

Prevention/Detection: Use a payroll list and visit Departments to verify existence of employees. Observe employee work stations or ask an employee who does not normally perform payroll duties.

The most common payroll fraud scheme is an employee who uses ghost employees to misappropriate funds. In some cases, these individuals actually complete application forms and are hired by the organization. Thus, there are legitimate personnel files on all employees. While these individuals perform no work, their time cards/sheets/lists are prepared to obtain payroll check payments that are then misappropriated. Collusion between employees is often required. Ghost employees represent an area within the payroll function that is often overlooked. So, what's the risk and why should you be concerned about it?

While you might find it hard to believe, most ghost employees are actually hired in the normal course of business. So, how can that be? In the largest case the State Auditor's Office has ever encountered, 13 ghost employees caused losses which exceeded $114,000. Since these individuals had actually been hired to work at the organization, they all had an official file in the human resources department. As a result, a test to determine if all employees on the payroll also have a personnel file will not necessarily detect a ghost employee.

In most typical ghost employee cases, the primary "red flag" encountered is that the **individuals never come to work**. But, the supervisor who hired these individuals still signs their time cards/sheets/lists (sometimes the employee's signature is not on the form) and approves them for payment. The supervisor then picks-up the payroll checks from the payroll function, distributes them to the individuals, and splits the proceeds from this illegal activity with them. When this event occurs, payroll checks are often endorsed by both parties, another "red flag". Where pick-up and hand delivery of payroll checks is a

standard payroll practice, this condition is a higher risk than if the checks are actually mailed to the employees or sent to their banks via electronics fund transfers. But, fraud can occur in either situation.

Temporary employees may also be used in ghost employee schemes. For example, a payroll supervisor or other key payroll official may take advantage of the large number of temporary employees used by the organization and leave them on the system after their employment has terminated. The **direct deposit bank account number** for these ghost employees is changed to match the payroll supervisor's or other key payroll official's direct deposit bank account number. Small amounts are misappropriated from each ex-temporary employee to avoid detection. This scheme usually requires the abuse of a large number of ex-temporary employees to misappropriate a large amount of money.

How do you detect a scheme similar to the above case scenarios? The ghost employee test is designed for this purpose and should be periodically performed by every organization. Conducting the test for all employees is one way to do this in small organizations. But this may be too costly and time consuming in larger organizations. Thus, conducting the test for all employees in a particular department, function, or activity is another way to complete this task. How is the ghost employee test conducted? There are two ways to perform this test.

(a) Conduct a **payroll payout**. All payroll checks (or electronic fund transfer documents) are obtained and distributed to the employees. This approach is not recommended because it can easily cause an unnecessary employee morale problem due to the timeliness of receipt of the funds, inconvenience about time of day or location of event, etc. The resulting complaints are never worth all the trouble.

(b) Use a **payroll list**. Obtain a list of all payroll transactions for a specific pay period. Visit the departments to conduct the test. Observe employee work stations or ask an employee who does not normally perform payroll duties (i.e.; does not process time cards/sheets/lists or leave slips) to review the payroll list and confirm that all employees actually work there.

What employee categories represent the highest risk? Probably at least the following:

(a) Part-time, seasonal, or temporary employees. These individuals are employed throughout the year in a variety of departments. But, they may be concentrated in the parks and recreation department or similar function such as swimming pools during the Summer months. Examples in school districts might include substitute teachers, custodians, and bus drivers. Thus, you might test these categories of employees during this period of time (i.e.; Summer).
(b) Employees who terminate employment at the organization. This could also involve employees in retirement systems. In these cases, no one notifies the organization when the individual dies. Or, after receiving the notification of death, an employee fails to process it and merely changes the individual's mailing address to one which they control, usually a post office box. Thus, improper payments continue to be made even after the death of the individual. The primary

test to perform is to determine if there are any payments recorded in the system after the termination date or date of death.

The reason these two categories are the highest risk is that organization procedures for terminations may not be very effective. Since these individuals already have been hired and have a personnel file, a department supervisor only needs to submit a time card/sheet/list for the individual (falsification of records) in order to obtain the funds from this scheme. Hopefully, ex-employees will complain about any pay irregularities when they receive their annual Internal Revenue Form (IRS) Form W-2. This feedback is an important part of any internal control structure. But, this may not actually occur unless the individual maintains accurate records on their own pay. Since this isn't always the case, a small overpayment amount per employee may not be noticed at all. The key is preparation, distribution, and reconciliation of the payroll processing system (IRS Form W-2's) to the organization's total payroll (IRS Form W-3's).

CASE EXAMPLES

The supervisor of transportation in at Tacoma School District stole $114,400 (1983) by using **ghost employees**. The district contracted with a public transit system to transport students to and from school. These bus drivers requested that bus monitors be placed on the buses to handle student discipline. The supervisor of transportation hired bus monitors through the district personnel system, including **13 individuals who performed no work**. The supervisor of transportation both completed and approved their time sheets. When payroll warrants were received, each person paid the supervisor of transportation a percentage split of their false wages. While the internal control questionnaire for the payroll function indicated that all payroll checks were mailed directly to the employees, the supervisor of transportation picked up these 13 checks at the payroll department at the end of each pay period (i.e.; "I go right by their house on my way home."). When one of the bus monitors decided that he no longer wanted to share the proceeds of this scheme, the supervisor of transportation pistol-whipped him and sent him to the hospital. Auditors found out about this fraud by reading the newspaper when the individual confessed this crime to the police and the press from his hospital bed. The supervisor of transportation received a tough prison sentence for the weapons charge. If a ghost employee check had been made at this district, no one in the bus monitor section could have verified the existence of these 13 employees because they never reported for duty.

A secretary at Methow Irrigation District stole $191,700 (1986-87) over a nine year period in a cash disbursement scheme by issuing prenumbered checks for claims payments to 20 fictitious companies ($163,800) and for **payroll to fictitious employees** ($27,900). Claims and payroll documents were altered after approval by the governing body. Fraudulent payroll transactions included additional payroll for herself (duplicate payments) and payments to **four fictitious employees**. Refunds were obtained each quarter (Form 971) from the Internal Revenue Service for the withholding amounts applicable to the fictitious payroll activity. There was no system of internal control because one person acted with absolutely no management review or oversight in the cash receipt and cash disbursement functions. She embezzled an additional $54,300 in cash

receipts. This involved 100% of all revenue received at the District. All other tax revenues went directly to the County Treasurer.

In 1988, the Government of Sierra Leone (West Africa) had a tremendous financial crisis. Annual expenditures were too high. When they performed **a census of all national employees, they found 9,185 ghost employees on the payroll (1 out of every 7 employees)**. Bogus pay checks were being pocketed by corrupt employees.

In September 2001, the British Broadcasting Corporation (BBC) reported that the government in the Democratic Republic of Congo has found that some 20,000 people were drawing civil service salaries without having jobs. In an interview with the BBC, Benjamin Mukulungu, the civil service minister, stated that the fraud had cost the government several million dollars. The government found out about the scam when auditors compared the government payroll with staff lists and found that about 20,000 people drawing salaries were not working for the government. Fraud in the Congolese civil service ha long been a problem, since the days when the Zairean dictator Mobuto Sese Seko would appoint friends and relatives to nominal government jobs.

(2) **Mid-month payroll draws not deducted from end-of-month payroll**.

> Attributes: (a) Occurs in small organizations. (b) More than one payroll draw per month. (c) Blank, void, or loss-leader warrants/checks are used for the unauthorized transaction. (d) An unauthorized adjustment must be processed, usually at the end of the month, to record the extra payment in the accounting system.
>
> High risk employee: (a) Payroll Department employee or manager.
>
> Prevention/Detection: (a) Review the payroll record of Payroll Department employees and managers. (b) Review the number of payroll payments per employee per month.

This payroll fraud scheme is perpetrated by a trusted employee who has complete control over the payroll function. This individual may be either the only person employed in the function, or the only person employed in the organization. Positions commonly involved in fraud cases have been the clerk-treasurer, business or office manager, controller, and payroll clerk.

When fraud occurs in this situation, the employee takes a mid-month payroll draw on their monthly salary, but does not subsequently deduct this advance from their end-of-month payroll entitlement. In one case, the employee's credit union deductions were also not deducted from their end-of-month payroll warrant. A variation of this scheme occurs when the individual deducts the wrong (lesser) payroll draw amount from their end-of-month payroll. In all cases, a payroll overpayment is the end result. We have also seen this variation used to make restitution to the organization for prior overpayments. When this occurs, the individual withholds the wrong (greater) payroll draw amount from their end-of-month payroll to make the repayment.

While **only one** payroll draw may be authorized by organization policy and state law, multiple payroll draws often occur in fraud cases. In one case, mid-month payroll draws actually exceeded the employee's total net pay for the month. These extra payroll transactions must be manually prepared and are concealed in the accounting records by indicating that the warrant was a "void" or by indicating an incorrect amount for the transaction. In one case, unnumbered (blank) warrants were used to conceal these irregular transactions. Accounting records are either falsified or altered to accomplish this act. An adjustment must be processed (usually at the end of the month) to record the extra payroll payment in the accounting system. This makes sure that the accounting records reconcile with the amount of cash in the bank.

CASE EXAMPLES

A controller in a hospital district and a business manager in a school district stole $800 and $2,130, respectively, by authorizing excess payroll disbursements for themselves. In the hospital district case, the controller took periodic payroll advances and then failed to repay the hospital through subsequent deductions from his regular payroll entitlement. In the school district case, the business manager took mid-month payroll draws from her normal salary, but failed to deduct these interim payments from her end-of-month payroll entitlement. Blank checks were used for the mid-month payroll draw transactions. These are good examples of cases where the individuals perpetrated more than one type of fraud at the same time. When answering the question: "What else does this person do?", the auditor found that: (a) the hospital district controller also used a district credit card to purchase items for his own personal use ($2,000 in additional losses); and (b) the school district business manager wrote checks to herself from two imprest fund checking accounts, used a district credit card to purchase items for her own personal use, and stole lunchroom cash receipts which were transmitted to her for deposit ($16,600 in additional losses).

An office manager in a transit system stole $2,400 by authorizing excess payroll disbursements for herself. She also took mid-month payroll draws from her normal salary. However, the end-of-month payroll register was altered to delete credit union deductions and mid-month payroll advances for herself. Overpayments were made when the transit system disbursed funds to the office manager for mid-month payroll draws and to the credit union for the office manager's payroll deduction. Payroll checks were also issued to the office manager in amounts greater than actually recorded in the payroll register.

(3) **Unauthorized employee pay**.

Attributes: (a) Fraud is usually not systemic. (b) It's a specific employee who manipulates their own payroll records.

High risk employees: (a) Department timekeepers. (b) Department managers. (c) Payroll Department employee or manager.

Prevention/Detection: (a) Monitor payroll records for key employees. (b) Review payroll records for unusual patterns for overtime, stand-by time, call-back time, regular hours, compensatory time, sick leave, and annual leave. (c) Look for a straight line from source to approval to payment. (d) Determine whether the organization has and properly uses compensatory time for employees. Transactions must be recorded.
Prevention/Detection: Determine if payroll checks/warrants are negotiated/cashed prior to pay date or by an unauthorized individual by reviewing endorsement information.

Unauthorized employee pay fraud schemes occur in a variety of categories, including irregular pay for overtime and stand-by or call-back time, regular hours, compensatory time, and annual and sick leave. These frauds are **usually not systemic**, but rather are committed by **specific employees** to obtain unauthorized pay for their own personal benefit. This often results in the employee receiving more pay than is authorized. However, in certain instances, fraud occurs when organization managers direct employees to file false time and attendance records to obtain funds for other unapproved purposes. Abuses have included the following: (a) Giving an employee a pay raise by allowing fictitious overtime charges because the pay raise could not be obtained through other authorized means. (b) Filing false payroll transactions to obtain funds to pay for student tuition and moving costs that could not be legitimately reimbursed by the organization. And, (c) Obtaining funds from federal grantors for use within the organization for purposes that are not authorized in the grant agreement. In addition, managers are usually prohibited from receiving overtime by organization policy. Therefore, overtime for this category of employee must be reviewed carefully. Other payroll manipulations most frequently occur in the payroll office because the employees who perform these tasks, particularly those in small entities, are in a position to circumvent organization policies for their own personal benefit. The same condition exists for the timekeeper in a Department or function of a large organization. Thus, managers and auditors should specifically review the payroll records for these individuals for any irregularities.

A supervisor, or other designated individual for managers at the top of the organization, should approve all employee time cards/sheets/lists and forward the documents directly to payroll for payment. These documents should never be returned to the employee. Our largest payroll fraud case occurred because an employee submitted his own time card/sheet/list without approval. It contained false entries for overtime and stand-by or call-back time hours which were never worked (49,000 hours over a 19 year period of time). This individual was a high level supervisor in the organization whose time was not monitored by the chief administrator. This clearly illustrates why no one should approve their own time and attendance record. In addition, when an employee works in more than one department, one supervisor should be designated to approve the individual's time sheet. The employee's time worked in another department should be verified with the supervisor in that department prior to certifying the payroll for payment.

(a) Overtime and stand-by or call-back time. Employees falsify overtime and stand-by or call-back time for hours they did not work, usually after their time

card/sheet/list has been approved by a supervisor. The employee completes unused blocks on the form when the supervisor returns the time card/sheet/list to them for further processing. The document is then forwarded to payroll after alteration (forgery). Thus, both managers and auditors should look for a **straight line** in processing from source to approval to payment. Employees file false time cards/sheets/lists without the fear of detection when no one approves their time and attendance record prior to payment. Overtime and stand-by or call-back time payroll fraud schemes are often hard to prove because there are no supporting documents to review after-the-fact. In these cases, procedures have not been established to use forms for advance approval of overtime to be worked that specifically identify the date, hours, and reason for the action.

(b) Regular hours, compensatory time, and sick and annual leave. Employees falsify their time cards/sheets/lists for these categories of work, usually after approval by a supervisor. But, they often forge the supervisor's signature on their time and attendance records to accomplish this act. Unauthorized work hours are added to time cards/sheets/lists, while sick and annual leave time actually taken is omitted from the document. Managers must have sufficient knowledge of the employee's actual work schedule to properly perform the payroll approval function. The organization must have a policy for compensatory ("comp") time. All comp time earned and used must be recorded in the payroll system, and maximum limits should be established similar to sick and annual leave balances. Comp time use and "buy-outs" must be made pursuant to organization policy.

Managers and auditors should use any alternative record available within the organization to assist in determining if timekeeping irregularities exist once the accuracy of an employee's time and attendance records have been questioned. The evidence for payroll irregularities, in priority order, includes:

- The time and attendance record.
- Outside documents that prove the case, such as airline travel tickets used during a period of time when work was claimed.
- A contemporaneous record kept by an employee whose job includes keeping track of things like leave. This record is usually the employee's personal calendar pad/book annotated with the leave information for one or more employees in the work unit.
- Statements of co-workers who use their time cards/sheets/lists as support to verify what they have said. Normally, the time and attendance records of others have nothing to do with the work of another. But, there are exceptions, such as when several employees participate in the same event. The critical factor is to link these documents together for evidence in any case.

- Other documents, such as appointment schedules, e-mail, telephone, travel vouchers, credit cards, purchasing documents, correspondence, etc.

The objective in any investigation would be to determine what type of "imprint" the individual would make at the office if they were present on a specific date. For scheduled events involving several employees, one employee's time and attendance record might be compared to the time and attendance records of other employees for agreement. Interviews with these other employees would also have to be documented to support any irregularity.

(4) **COBRA program abuses**.

Attributes: (a) Employees or dependents provided health and medical benefits without authorization. (b) Length of time employee is on the program exceeds limits authorized by law. (c) Payroll Department does not have a system to reconcile authorized payments to be received versus actual payments made to insurance carriers.

High risk employees: (a) Payroll Department employee or manager. (b) Organization manager.

Prevention/Detection: (a) Reconcile suspense funds established to process program payments. (b) Establish computer edits or manual controls to ensure no one remains in the program longer than allowed by law. (c) Establish procedures to ensure all participants are authorized and approved for the program by management. (d) Review payment records to ensure health and medical benefits are continued in force only for eligible individuals.

The federal Consolidated Omnibus Budget Reconciliation Act (COBRA) law gives employees and covered dependents the right to continue employer-provided group health coverage on a self-paid basis for up to 18 months (and in some cases up to 36 months) after the individual would otherwise lose eligibility.

However, the COBRA program makes the Payroll Department a **cash receipting function** for these ex-employee payment transactions. Thus, there is a **hidden danger** here because few people realize that money flows through the Payroll Department. In this program, ex-employees pay their insurance premium to the organization to continue their health/medical benefits in force after termination. These individuals personally pay this cost directly to the organization until they are able to obtain other employment and other insurance coverage at their new employer or until the expiration of the COBRA program participation.

Ex-employee COBRA payments are processed within the Payroll Department in two ways: (a) Checks are made payable to the organization, deposited, and the amount included in the organization's payment to the insurance carrier. (b) Checks are made

payable to the insurance carrier, but processed through the Payroll Department for verification of payment and then transmitted to the insurance carrier with the organization's payment.

Payroll Department employees commit a variety of irregular acts in the COBRA program to obtain funds for their own personal benefit.

(a) Payroll Department employees steal payment checks from ex-employees who pay the organization for their health/medical benefits (i.e.; checks made payable to either the organization or the insurance carrier). In these cases, the organization does not properly monitor the COBRA program to prevent this abuse. Thus, they subsequently pay the premium for the benefits of these individuals even though no funds have actually been received (i.e.; no money in, but money out). Employees deposit these checks in their own personal bank account or in non-public bank accounts maintained within the organization that have similar sounding names. This makes depositing these checks easy. Once funds are deposited in these checking accounts, the employees write checks to themselves, to "cash", or pay their own personal bills directly from the bank account.

(b) Payroll Department employees also steal warrants the organization has issued to the insurance carrier that provides these health/medical benefits for the employees. Hopefully, these irregularities are promptly noted by the insurance carrier and resolved by someone within the organization other than the perpetrator (an independent party).

(c) In one case, a computer programmer altered a computer record to extend an ex-employee's benefit termination date without authorization. The individual was a friend, and the record alteration was processed as a favor from one employee to another.

(d) In another case, a dependent of an employee was provided health/medical benefits without authorization.

Organizations should: (1) Reconcile suspense funds established to process COBRA payments. An agency fund using the zero balance accounting procedures may be used for this purpose. (2) Establish computer edits or manual controls to ensue that no one remains in the COBRA program longer than allowed by law. (3) Establish procedures to ensure that all participants are authorized and have been approved for the COBRA program by management. And, (4) Review payment records to ensure that health/medical benefits are continued in force **only** for eligible individuals.

(5) **Advance release of withheld funds**.

Attributes: (a) Payroll warrants/checks are issued prior to pay date. (b) Payroll warrants/checks are endorsed prior to pay date and by an unauthorized individual.

High risk employees: (a) Payroll Department manager. (b) Chief financial officer of the organization.

In this payroll fraud scheme, key financial managers in the organization disburse funds that have been withheld from employee payroll to an interest-bearing personal bank account prior to the due date required by federal and state agencies (i.e.; early deposit). These funds are then transferred to the correct bank account on time. The unethical financial manager takes advantage of the deposit delay to obtain a personal benefit from the interest received from the bank while the organization's withheld funds are maintained on deposit in their own personal bank account. There have been no cases of this type of fraud in the State of Washington as of the date of this writing (December 2001). However, this type of fraud has been detected in the private sector. The bottom line is that this type of fraud could occur anywhere. Therefore, managers and auditors should be alert for this irregular condition.

Red Flags:

Inappropriate employee segregation of duties.

Management officials or internal auditors do not periodically perform a ghost employee test.

Total payroll expenses exceed the amount of payroll reported on W-2 and W-3 forms filed with the Internal Revenue Service (IRS).

The quarterly Form 971 filed with the IRS indicates routine refunds (i.e.; over-deposits) to the entity.

Payroll checks are issued to individuals for large or even dollar amounts.

Managers do not verify that mid-month payroll draws are deducted from end-of-month payroll. This primarily applies to small organizations.

Excluding overtime, total payroll for key entity employees exceeds the authorized level.

Employee time sheets are returned to the preparer (source) after approval rather then sent directly to the payroll function. The entity should use the "straight line concept" where all transactions go directly from source, to approval, to payment.

Excessive overtime wages are reported for certain employees.

Time sheets or other time records are not signed by the employee.
Payroll checks are endorsed by more than one person.

Retirement checks returned as undeliverable by the post office are held in the retirement system office and are not dealt with promptly.

Checks for retirement fund withdrawal transactions are returned to the retirement system office for distribution.

An address change in a retirement account is immediately followed by a request for payment.

Fraud Detection:

Perform a ghost employee check either by: (a) making an actual payroll pay-out where all employees must present themselves and proper identification before receiving their checks (not recommended); or, (b) by taking the most recent payroll list to each department or function and having someone who does not perform any payroll duties verify that the employees actually exist (preferred method).

Determine that all mid-month payroll draws are authorized and have been deducted from end-of-month payroll entitlements.

Review overtime procedures for propriety, and analyze excessive overtime worked.

Determine whether any employees annual salary exceeds the authorized level.

Analyze Forms W-2 and W-3 filed with the individual and the IRS, respectively, for any unusual attributes or irregularities.

CASE EXAMPLES

Harborview Medical Center – Clinical Engineering Department ($1,902)

Elements of the Fraud.

(1) Employee's father arranged for her temporary assignment as a secretary in the Clinical Engineering Department, by-passing standard hiring practices.

(2) For three pay periods, the employee had her supervisor approve her time sheets. The time sheets were subsequently returned to the employee where additional hours were added which were not worked.

(3) For three pay periods, the employee forged the supervisor's signature on her time sheets and claimed more hours than were actually worked.

(4) The employee's father approved one of her time sheets with hours documents which were not worked.

Red Flags.

(1) Management oversight over time keeping for temporary employees was limited. Review of the department budget was not performed in a timely manner.

(2) Time sheets were returned to the employee after approval. This was a secretary who was r responsible for sending time sheets to payroll.

(3) Payroll did not monitor approval signatures, as evidenced by the father being able to approve her time sheet.

Detection Techniques.

(1) Determine what employees would be at risk (secretaries, timekeepers, supervisors). Review overtime reports on these individuals. For those with significant overtime, ask their supervisor if the overtime reported is reasonable and appropriate.

(2) Through CAATS testing, determine: (a) Who are the "big winners" in overtime, in terms of total dollars, and/or as a percentage of total salary; (b) Which salaried managers are being paid overtime (usually not eligible for overtime).

(3) Test individual overtime while performing tests of payroll. Always trace back to department records if possible, and inquire of the supervisor as to reasonableness.

University of Washington Medical Center - Cardiac Diagnostic Services Department ($264,563)

Elements of the Fraud.

(1) A Manager falsified his own payroll records for 19 years (1974-1993) for overtime and stand-by time that he never worked. The amount of fictitious overtime was $203,671. The amount of fictitious stand-by time was $60,892.

(2) A Manager's overtime exceeded 25% of his base salary in violation of University policy for 14 of the 19 years.

(3) There was an inappropriate segregation of duties. The Manager was responsible for preparing and approving payroll documents.

(4) The Department did not monitor compliance with the University's policy regarding overtime payments in excess of 25% of an employee's base salary. A University policy was not programmed as a computer edit for review purposes.

Red Flags.

(1) The Manager's exception time report was only signed by the employee. It was not approved by his Supervisor (blank approval box on the form).

(2) The Manager was a salaried employee and was not entitled to any overtime payroll payments.

(3) The Manager was a salaried employee. He was neither scheduled for nor performed any stand-by duties. He was not entitled to any stand-by payroll payments.

(4) Original exception time reports indicated overtime and stand-by time, but Department copies of the forms indicated only regular hours worked.

(5) The Manager's personal time record (UW Form 220) indicated only regular hours worked.

Detection Techniques.

(1) Select all employees receiving overtime and stand-by time payments. Sort from highest to lowest. Those at the top of the list are usually the highest risk employees for abuses of these payroll programs. Verify eligibility for overtime and stand-by time payments. Salaried employees are normally exempt from these types of payments.

(2) Select all employees receiving overtime and stand-by time and verify eligibility for this special pay. Sort from highest to lowest. Compare selected names to authorized stand-by records and designated positions.

(3) Review overtime records for compliance with University policy that no employee may receive more than 25% of their base salary without specific approval. Determine the entity's method of verifying compliance with this policy.

(4) Use only original source documents for audit testing purposes (i.e.; payroll copy of exception time reports).

(5) Compare employee's personal time records to payroll exception time reports for agreement.

PAYROLL FRAUD CASES

Washington State Auditor's Office
January 1, 1987 through December 31, 2003

Category	No. of Cases	Loss Amounts
Mid-Month Payroll Draws	5	$ 8,037
False Overtime and Stand-by or Call-Back Time	8	379,610
COBRA Manipulations	5	58,759
Payroll Office Manipulations	7	94,615
Payroll Abuse by Managers	5	113,146
Employee Time and Attendance	44	198,623
Total Payroll Frauds	74	$ 852,790
Percentage of Total Frauds	12.5%	7.0%

PAYROLL FRAUD CASES

Washington State Auditor's Office
January 1, 1987 through December 31, 2003

AMOUNT DESCRIPTION

Mid-Month Payroll Draws.

$ 450 Washington State Substance Abuse Coalition (1999). The Executive Director took payroll advances and did not deduct them from her end-of-month check and was paid twice for the same vacation pay.

2,241 City of Battle Ground (1997). The Clerk-Treasurer and Utility Clerk were overpaid in payroll. Mid-month payroll draw procedures were violated when more than one draw was taken (7 times in 2.5 years). Mid-month payroll draws were not deducted from end-of-month payroll, or were deducted in the wrong amounts. In one instance, mid-month payroll draws exceeded the employee's net pay for the month. These extra payroll transactions were manually prepared rather than computer produced, and were signed by the individual receiving the funds (Clerk-Treasurer). **The payroll warrant register was falsified** to conceal these transactions in two instances. One transaction was posted as a "void" while the amount of another transaction was altered to indicate an incorrect amount.

816 Adams County Hospital District No. 2 (1991). The controller took periodic payroll advances and then failed to repay the hospital through subsequent deductions from his regular payroll entitlement. He also made unauthorized credit card purchases for his own personal use totaling $1,961.

2,400 Pacific Transit System (1988). The office manager took mid-month payroll draws, but omitted the draws and credit union deductions from her end-of-month payroll check. The end-of-month payroll register was **altered** to delete credit union deductions and mid-month payroll advances made. Payroll checks were issued to the office manager in amounts greater than actually recorded in the payroll register.

2,130 North Beach School District No. 64 (1987). The business manager took mid-month payroll draws from her normal salary, but failed to deduct these interim payments from her end-of-month payroll check. **Blank (unnumbered) checks** were used for the irregular mid-month payroll draw transactions. She also misappropriated an additional $16,768 by stealing lunchroom cash receipts, writing checks to herself from two imprest fund checking accounts, and using the district's purchasing credit card to buy items for her own personal use.

$ 8,037 5 Cases -- Mid-Month Payroll Draws

False Overtime.

$ 8,832 University of Washington Medical Center (2002). A Nurse in Materials Management claimed stand-by time from the time she left work until the time she began he next shift because she had been asked to wear a pager. The employee was on temporary appointment in one Department but submitted the time sheet to the home Department for approval where they had no direct knowledge of her work schedule or hours actually worked.

30,589 University of Washington (2002). An employee in the Diabetes Endocrinology Research Center was granted a salary increase without proper authorization. Rather than request a reclassification of the employee's position, managers authorized the employee to add 8 hours of overtime to each month's time sheet. This lasted 16 years under four different Center managers, and involved false time sheets, work and leave records, exception time reports, and federal grant certification reports.

3,510 Harborview Medical Center (2002). A hospital assistant in UW Medical Center Rehabilitation Services received overtime for hours not worked for 3 months. The employee's time sheet was falsified using "white-out", and by changing the amount of hours worked after supervisory approval.

52,723 Benton County public Utility District No. 1 (2002). A Branch Manager falsified his time sheet for over 3 years to show that he worked stand-by hours that other District employees actually worked. He paid the other employees in cash for the hours they worked. The District incurred excessive payroll expenses and the Manager falsely increased his retirement benefits because the Manager's rate of pay was higher than the other employees.

4,140 City of Olympia (2001). A Public Works Department employee was paid overtime for time not actually worked (six hours per pay period for over a year). Unable to obtain a pay raise for the employee using normal City procedures, supervisors allowed the employee to file false overtime in compensation for working out of his job classification.

189 City of Pateros (1996). The City Clerk issued extra payroll draws to herself based on unapproved overtime claims. Time sheets were not signed by the supervisor (Mayor), and 4 contained a **forged** signature. Two days of leave were taken but not recorded in city accounting records.

264,563 University of Washington - Medical Center (1993). A supervisor falsified payroll records for 19 years for 49,000 hours of overtime and standby time which he never worked. He also **approved his own time sheet**. The overtime exceeded 25% of his base salary in violation of University policy in 14 of these years (policy was not reviewed or enforced).

15,064 University of Washington - Department of Medicine (1993). A secretary falsified her own payroll records to obtain overtime for hours she did not work. Payroll records were **altered after supervisory approval**, and supervisory approval signatures were **forged**.

$ 379,610 8 Cases -- False Overtime and Stand-By Time

COBRA Manipulations.

$ 228 Lake Stevens School District (2001). A payroll specialist did not deduct a medical insurance premium from her paycheck even though the District paid the fee to the insurance plan administrator. The employee altered her payroll deduction codes for personal reasons. The District did not reconcile insurance premium receipts to insurance company providers in the COBRA program.

4,499 Housing Authority of the County of King (1994). A payroll clerk issued checks to herself from an employee association bank account. To conceal this activity, COBRA payments made by ex-employees were deposited into the employee association bank account (similar account names). Health care premiums were paid for all individuals.

-0- Health Care Authority (1993). A computer programmer in the Department of Personnel accessed a computer record without authorization and modified the COBRA benefit termination date of a former employee of the Health Care Authority. A Health Care Authority system security officer shared his computer password with the computer programmer who used it to process this unauthorized transaction. Computer edits were not properly programmed in the system.

2.355 Grant County Hospital District No. 4 (1992). Two hospital administrators made unauthorized disbursements to themselves for dependent insurance premiums and personal expenses for travel and telephone.

51,677 Kent School District No. 415 (1992). A benefits technician in the payroll office stole payment checks from COBRA and leave of absence employees (personal payment of medical benefit premiums). The district subsequently paid for these benefits (no money in, but money out). She also stole district warrants issued to various insurance companies.

$ 58,759 5 Cases -- COBRA Manipulations

Payroll Office Manipulations.

$ 9,229 South Whidbey School District (2003). A Payroll Officer falsified her own payroll records to increase her pay through unauthorized means. As a result, the District paid her personal obligations at three financial institutions as well as her medical premiums. In addition, she increased her own new pay by recording negative employee deductions.

21,607 King County-Medic One Program (2003). A Fiscal Specialist manipulated payroll records to misappropriate funds for herself and her daughter through improper payroll disbursements over a period of three years. These improper payments included unauthorized overtime, regular pay misclassified as overtime, payment for time not worked, and payment at more than the authorized pay rate.

4,500 Kent School District (2002). The Supervisor of Accounting and Payroll made test entries in the payroll processing system that resulted in discrepancies in his own payroll records for 3 years. The District overpaid the IRS for federal withholding taxes. The employee's reported federal withholding taxes were overstated by $4,500 and his reported federal taxable wages were understated by $20,500.

17,888 City of Tenino (1997). The Clerk-Treasurer issued a duplicate payroll check to herself for one pay period. She also issued checks made payable to herself from the city's checking account. The check register was incomplete and inaccurate, and had been altered to delete these irregular checks **(falsification)**.

5,000 University of Washington - Payroll Office (1995). A temporary employee (minor) made two payroll checks payable to a friend and falsified the approval signature **(forgery)** to get the checks signed and issued.

17,190 Tacoma Metropolitan Park District (1995). A Payroll Officer falsified accounting records to manipulate payroll records for the benefit of herself and others. A friend was overpaid by changing the rate per hour of work, and paying for vacation and military leave for which the individual was not entitled. Several other employees paid a medical aid rate less than authorized by law, and she manipulate her own pay by reducing the federal withholding and state retirement amounts. The employee added 8 hours of vacation pay to her time sheet **after supervisory approval**. This alteration was detected and led to her dismissal.

19,201 City of South Bend (1994). The Clerk-Treasurer paid herself extra payroll checks and manipulated other transactions for vacation, sick leave and compensatory time buy-outs. Normal payroll checks were signed by the Mayor; however, the irregular payroll checks were signed by using a facsimile signature stamp **(forgery)**.

$ 94,615 7 Cases -- Payroll Office Manipulations

Payroll Abuse by Managers.

$ 7,427 Ocosta School District (2002). While the Vocational Education Department Director did not attend assigned meetings for a decade, she was paid for time spent at meetings because the District believed it was properly represented. These wages were not earned.

$ 1,640 Washington State Substance Abuse Coalition (1999). The Executive Director paid herself twice for the same vacation pay.

34,855 Town of Rosalia (1997). Town officials **knowingly falsified time records** to indicate police duties were performed by a maintenance person in order to obtain federal grant funds in the COPS Fast Program. Salary and benefits charged to the grant were not always supported by time and attendance records, and some charges were based on percentage allocations rather than actual hours worked.

51,455 University of Washington - Regional Primate Research Center (1995). An administrator **directed the fiscal specialist to falsify payroll records** so three students would receive a sufficient amount of funds for their tuition. The students performed no work.

17,769 University of Washington - Regional Primate Research Center (1995). The director **directed an employee to falsify payroll and travel expense**

records to compensate 3 students for moving costs and 1 student for tuition. Payments for work prior to the student's actual start dates and payment for a non-existent travel event were used.

$ 113,146 5 Cases -- Payroll Abuse by Managers

Employee Time and Attendance.

$ 745 University of Washington Medical Center (2003). A Nurse used taxi transportation services for personal purposes on 33 occasions for a total of $441 over a 20-month period. Comparison of transportation orders to the employee's timesheets revealed that the Nurse was picked-up prior to her normal quitting time. Thus, the Nurse was paid for services not rendered on 13 occasions totaling $745 plus related benefits.

1,525 University of Washington Medical Center (2003). A Hospital Assistant was paid for services not rendered over an 18-month period. The employee reported work the same day and time in two Departments on seven occasions. On five occasions, the employee used sick leave benefits in one Department while working in the other Department. On 15 occasions, the employee reported the same quitting time in one Department as the starting time in the other Department even though these two Departments were located in different parts of the city.

603 University of Washington Medical Center (2003). A Hospital Assistant deposited another employee's payroll check into her own personal bank account. The employee claimed this was a careless mistake.

102 Tacoma Community College (2003). A Work-Study Student employee misrepresented the number of hours worked by forging his supervisor's signature on three timesheets.

2,443 Lake Washington School District (2003). An elementary school Night Custodian received compensation for 162 hours and 46 minutes not worked for almost one school year. The school's security system documented that the employee left work early on numerous occasions, and claimed eight hours of work on five separate days when a substitute custodian worked in his place.

10,627 Town of Kahlotus (2002). The Clerk-Treasurer claimed monetary compensation in lieu of receiving medical insurance coverage while enrolled in the medical insurance plan, thus receiving a double benefit. The employee received family medical coverage when Town medical coverage is only for employees. The employee issued a payroll check to herself to $500 more than approved by the Council.

1,056 Town of Ruston (2002). The Police Chief claimed compensation for hours not worked on 2 occasions. He falsified his time sheet to indicate he

was working when he was scheduled to attend a one-week training class that he did not attend and was teaching afternoon classes at a state community college.

173 City of Bellingham (2002). A cemetery employee was overpaid one day of wages for hours not worked.

29,452 Thurston County Cemetery District No. 2 (2002). The Cemetery Caretaker submitted fictitious payroll claims to the County for payment without approval by the Commissioners for 4 years.

17,482 University of Washington Medical Center (2002). A Registered Nurse in Surgical Services received compensation for time not worked. The Department submitted time sheets indicating leave without pay. However, the proper personnel action forms were not submitted and records in payroll records. The employee did not notify the University of the unearned payments.

12,389 University of Washington Medical Center (2002). A Medical Interpreter in Interpreter Services received compensation for time not worked. The Department submitted time sheets indicating leave without pay. However, the proper personnel action forms were not submitted and records in payroll records. The employee did not notify the University of the unearned payments.

449 Clark Regional Emergency Services Agency (2002). An employee forged a doctor's signature and filed two false documents submitted as excuses for sick leave absences in order to receive payment for time not worked.

15,655 Washington State University (2002). An employee of the College of Business and Economics made fictitious claims for the payment of wages on two, non-existent, temporary appointments in 2000 and 2002.

546 Bellevue School District (2001) Two substitute custodians were paid for hours not worked (99.25 hours and 9 hours). The employees left work early and did not sign their time sheets. The District did not use alternative records (sign-out log and activation of the building alarm system) to verify the accuracy of the employee's time records.

2,285 Lake Washington School District (2001) A custodian did not make an accurate report of all time worked. The employee left work early and a supervisor did not sign the employee's time sheet. The District did not maintain adequate records of the starting and ending times of work for certain hourly classified employees.

266 City of Tacoma (2001). A financial assistant submitted a false claim for employee benefits. The original receipt from the medical provider was issued for $185, but had been altered claiming reimbursement for $485.

This fictitious transaction was detected by the City's third-party administrator who looked at other transactions for this employee. One paid claim was found that was not supported by a valid provider receipt. Rather, a fictitious receipt was created to obtain payment for these benefits ($266).

2,451 Washington State Library (2000). A fiscal technician falsified interagency leave transmittal documents by entering incorrect leave balances or by changing recorded leave balance information on these forms when transferring in and out of the Agency. In addition, the employee did not always record their own sick and annual leave transactions accurately in the Agency's official leave accounting system. The employee's leave balances exceeded actual entitlements by 179.6 hours.

913 Department of Licensing (1999). An employee intentionally collected salary for 70.8 hours of time that he did not work.

1,918 The Evergreen State College (1999). A student submitted two time reports to his supervisor which were approved for payment even though the number of hours worked was inflated (false). The student submitted two additional time sheets directly to payroll for time not worked and forged the supervisor's signature on the forms.

1,050 Washington State University – Department of Crop and Soil Sciences (1999). A student employee falsified 150 hours of work on his time sheet. The employee's time sheet was approved by a supervisor and returned to him. He then falsified the tie sheet by inflating his hours of work before it was forwarded to payroll for processing and payment.

1,471 Harborview Medical Center – Environmental Services Division (1999). A custodian supervisor worked full-time at the hospital and part-time at the Kingdome. In 34 instances, the employee recorded that he worked a total of 77.6 hours for both entities at the same time (i.e.; double billing of payroll). In five instances, time records were altered by using "white out".

5,097 Valley Medical Center – Operating Room (1999). An operating room nurse was overpaid. An employee security system recorded that the nurse was signed into the Fitness Center on 148 instances while he was still shown as working in the operating room. In 54 of these 148 instances, the employee's supervisor manually recorded the time the nurse left the operating room because the employee stated that he had forgotten to punch out using the official system. Overtime hours were manually recorded on the daily time tracking sheet by the nurse and were not approved by a supervisor.

1,912 University of Washington - Psychology Department (1998). Time sheets for three employees were falsified, and erroneous charges were made to federal research grants. Two time sheets were signed by someone other

than the employee. The research project did not track the accumulation and use of compensatory time for five employees.

2,730 University of Washington - Department of Pathology (1998). A student employee falsified his time sheet for 1.3 years and was paid for 420 hours he never worked on a federally funded research project. The student admitted that he had not obtained proper supervisory approval for his hours , but instead had signed an indecipherable name on his time sheets **(forgery)** to indicate supervisory approval during this time period. The department did not adequately monitor the work of students.

1,902 Harborview Medical Center (1998). A temporary employee in the Clinical Engineering Department falsified her time sheets and **forged** a supervisor's signature for 3 months. As a result, she was paid for 212.15 hours she did not work. When the supervisor actually signed time sheets, they were **falsified after approval** and then submitted for payment. The employee also retained all copies of the accounting documents which reflected these irregular payments in an attempt to conceal this loss.

2,964 Department of Social and Health Services (1996). An employee failed to record 205 hours of his own personal annual and sick leave in the personnel/payroll system. Segregation of duties problem with no monitoring of input and output documents.

3,373 Public Hospital District No 2 of Snohomish County (1996). A part-time nurse falsified the number of hours and shift worked on her time cards. **Work in two different units** complicated this case because only one supervisor signed the time cards. One unit was accurate while the other was falsified by 123 hours of work.

5,627 Everett Community College - Automotive Department (1996). An automotive instructor used college facilities, personnel, and other assets for private gain or benefit. He operated a private business involving use of a computer, fax machine, shop facilities, and time of other employees to run errands and service his car. The instructor did not perform all hours of work required by his contract.

2,535 Department of Social and Health Services (1996). An employee failed to record 172 hours of her own annual and sick leave in the personnel/payroll system. Segregation of duties problem with no monitoring of input and output documents.

1,586 City of Tacoma - Public Works Department (1996). The Division timekeeper altered her time cards **after supervisory approval** but before final processing by using white-out and write-overs. Twenty time cards and 55 hours of work were falsely reported.

-0- University of Washington - Pathology Department (1996). An employee falsified time sheets for herself and daughter on federal research projects. Time sheets signed by a supervisor were faxed to payroll and the employee signed her daughters time sheet. Duplicate and incomplete/inaccurate time sheets were also submitted. This case was complicated by **work in two departments** and approval by only one supervisor.

8,373 University of Washington - Computing and Communications (1996). An employee falsified his own time sheets. He later stated that he only worked about half the hours he reported. Building security access records indicated he worked only about 25% of the hours reported.

3,841 Harborview Medical Center (1996). The Ambulatory Care Services Administrator used his official position for private benefit. Abuses included personal cellular and long distance telephone use, shipping charges, and food expenses, as well as payment for 28 hours of time not worked (false time sheets). The employee was conducting a private consulting business during normal duty hours. Improper employee hiring and personnel transfer actions were also disclosed.

7,137 King County - Department of Information and Administrative Services (1996). A confidential secretary adjusted her hourly pay rate on payroll transmittal forms **after supervisory approval** and before submission to the payroll department. Losses included employer payroll taxes paid on the unauthorized salary amount.

718 Western Washington University (1996). A Physical Plant employee took time off but did not submit documents for 32 hours of annual leave and 2 hours of compensatory time.

6,437 Housing Authority of Asotin County (1996). The executive director received dual compensation for his regular salary and for disability benefits from the Department of Labor and Industries.

2,007 University of Washington - Experimental Education Unit (1995). A transition specialist conducted an unapproved private consulting business during normal business hours. He used University facilities, editing services, and telephones in the business operation, and failed to report or falsely reported his annual and sick leave.

2,500 Irvin Water District No. 6 (1995). An Office Manager was paid for 144 hours which were not worked (documented by management monitoring). After overpaying insurance premiums, the manager directed the company to apply the excess to a policy for her daughter.

1,585 University of Washington - Department of Metabolism (1994). A fiscal specialist processed fictitious petty cash vouchers for purchases and

services, used the state telephone system to make personal calls, and did not report at least a one day leave of absence to the University.

9,135 University of Washington - Applied Mathematics Department (1994). A department administrator processed fictitious petty cash vouchers, incurred unauthorized shipping charges for personal purposes, used the state telephone system for personal calls, and did not record all leaves of absence from the University. Miscellaneous cash receipts were also stolen.

460 Green River Community College (1993). A college student falsified college work study time sheets and **forged** a supervisor's signature to obtain fraudulent payments in two fiscal years. Student financial aid funds were involved.

1,734 University of Washington - Medical Center (1993). A fiscal specialist misapplied rules for leave accrual, misrepresented time worked, received both payment and time off for the same accrued compensatory time, did not deduct leave without pay from payroll time reports, and did not have leave records on file for 4 absences. Payroll records were also falsified.

184 Yakima County (1989). An Undersheriff filed duplicate wage and travel vouchers with the Washington State Criminal Justice Training Commission and Yakima County to receive more pay than authorized for services rendered.

23,185 City of Tacoma (1987). A Tacoma Dome manpower employee **forged** the name of supervisors and submitted false time sheets.

$ 198,623 44 Cases -- Employee Time and Attendance

$ 852,790 Grand Total (74 Cases) – 12.5% of all cases and 7.0% of all dollar losses

Payroll Analytical Procedures and Computer Assisted Audit Techniques (CAATs)

(1) Compare payroll expenditures from one year to the next in total and by department or function, and evaluate for reasonableness or established expectations (i.e.; cost of living allowances, change in FTE's, retirements, etc.). This analysis provides indicators of change and may identify areas of high risk for further payroll testing during the audit.

(2) Compare payroll expenditures to total organization expenditures from one year to the next. Determine the actual percentage of payroll expenditures and if it is consistent from year to year. This analysis provides indicators of change and may identify areas of high risk for further payroll testing during the audit.

(3) Summarize annual gross payroll amounts (excluding overtime) for all employees. Sort from highest to lowest. Determine if:

- Other than expected key officials are at or near the top of the list.
- The salary of key officials exceeds the authorized level.
- This test will detect mid-month payroll draws that have not been deducted from end of month salary.
- This test will detect employees with leave and contract buy-outs. Determine if these transactions were pursuant to contract requirements and organization policies.
- Specifically, this test should be performed for payroll department employees who occupy the highest risk positions and could falsify their own time card/sheet/list without detection by an unsuspecting supervisor or other approval authority, particularly in small organizations. It could also be performed for the timekeeper in a Department or function of a large organization.

(4) Compare annual gross payroll amounts and income tax withheld to IRS Forms W-2 (individual form) and W-3 (organization transmittal to IRS) for agreement. Under-reporting of payroll information to the IRS could be an indicator of fraud.

(5) Summarize wages for overtime, stand-by or call-back time, other non-regular pay types, and comp time for all employees. Sort from highest to lowest. Determine if:

- Amounts are excessive. In addition, the employees at the top of the list are the highest risk employees in the organization.
- Amounts exceed organization policy.
- Amounts are authorized. Salaried employees are not entitled to overtime or comp time. Employees receiving stand-by or call-back time must be in authorized positions and be on stand-by or call-back rosters/schedules for the time period involved.
- Accruals agree with organization policy and do not exceed authorized levels.
- Maximum year-end balances do not exceed organization policy unless specifically authorized by management and properly supported.

(6) Sort all payroll transactions from highest to lowest. Determine if any large transactions exist that are inconsistent with the expected list of key officials from (3) above.

(7) Determine if there are any changes in the pay rate beyond the expected cost or living adjustments, step increases or a selected dollar amount. Compare total payroll by employee from one year to the next, eliminating pay increases of less than a specified percent and dollar amount. Sort the remaining list of employees from highest to lowest. This list will identify new and terminated employees and could be used in lieu of the testing in (11) below. This list can be used to focus on all other unusual pay increases.

(8) Determine if any employee received more than one payroll payment per pay period or more than one payroll draw per month.

(9) Determine if any employee received a pay increase of greater than 10% in the same job class during the year.

(10) Trend payroll by month at various levels including total organization, departments, functions, etc. Identify months with anomalies and employees with unusual payroll activity in those months for further testing.

(11) Compare employee names in the payroll system from one year to the next for agreement. This identifies new employees and terminated employees for further testing purposes.

- For new employees, determine if pay rates agree with hiring documents in the personnel file.

- For terminated employees, determine if any payroll payments were made after the effective date of termination.

(12) Identify all employees in the payroll system with the same address as another employee in the employee file. An authorized exception would be for members of the same household. Verify information to personnel records.

(13) Sort direct deposit bank account numbers in the payroll system to determine if any duplicate numbers exist. An authorized exception would be for members of the same household who have the same direct deposit bank account number. Verify information to personnel records.

(14) Perform a variety of tests involving employee social security account numbers (SSAN). Contact Team STAT for assistance on these steps because they have the computer programs and files needed and can perform this work for you.

- Perform a validity check to determine if the numerical information meets authorized parameters for construction of the SSAN. This test could identify a ghost employee.

- Perform a validity check using the Social Security Administration's "dead" file to determine if the member is deceased.

- Perform a validity check to determine if the SSAN could not belong to the employee listed in the file based on birth date (e.g.; SSAN was issued before the person was actually born). The file used must contain the SSAN and the birth date of employees tested.

- Sort SSAN's in numerical order and perform a count to determine if duplicate numbers exist (i.e.; number cannot appear in the payroll system more than once). If so, identify all employee names associated with each number.

(15) Compare the COBRA program start date and current date to determine the length of time of program participation by ex-employees to ensure that program limitations have not been exceeded.

Other Payroll Attributes and Audit Tests

(1) Perform a ghost employee check by taking the most recent payroll list to each department or function and having someone who does not perform any payroll duties verify that the employees actually exist. Coordinate this test with other Department audit work.

(2) Determine if all mid-month payroll draws are authorized and do not exceed the organization's policy.

(3) Look for a straight line from source to approval to payment for payroll transactions.

(4) Scan time cards/sheets/lists for a specified period to determine if all employees have signed the documents and if all documents have been signed and approved by a supervisor.

(5) Determine if there are any payments made to an employee for work performed after the date of death or date of termination of employment with the organization.

(6) Determine if all ex-employees who participate in the COBRA program are eligible for the program, and whether required monthly payment amounts have been received from each participant.

(7) Determine if the organization promptly reconciles the suspense fund established to process COBRA program payments by participants.

(8) Review the bank endorsements on warrants transmitting all funds withheld from employee's pay to the organization's bank for payment to the Federal Government. Review the bank date of processing to ensure that funds were not disbursed before the required due date. Review the bank endorsement to ensure that funds were deposited in the proper bank account. Review the date and bank account information on similar documents used for electronic funds transfers of these funds.

(9) Determine if the payroll distribution reports or equivalent records are provided to appropriate Department personnel for review. Evaluate the effectiveness of this review. Remember that the concern is what was processed by the payroll processing system (e.g.; payroll register), not what was recorded on time cards/sheets/lists, and supposedly was input into the processing system.

ELECTRONIC FUNDS TRANSFER SCHEMES

This is an area that is often misunderstood by auditors and managers. The most frequently asked question by managers and auditors is: "Do I have to be concerned about the system itself?" The presentation below addresses this concern.

Problem: Banks use EFT's to move more than $1 trillion in funds around the globe each week, and the amounts are rising. Because of the large volume of transactions processed through EFT systems, they represent a prime target for fraud perpetrators who use "smash and grab" schemes and techniques to obtain an immediate, enormous source of money. Thus, these systems deserve the highest priority for security measures. While governments traditionally have used EFT transactions for investment purposes and automated clearing house (ACH) transactions for payroll payments, changes in technology will result in an increased level of disbursements being made through the EFT system in the future. When fraud occurs, employees first create and process fictitious electronic transactions inside the organization, and then process them through the EFT or ACH systems.

Solution: The bank's EFT and ACH systems are not the source of your risk. Rather, you must focus inward on employees who create and process these transactions within the organization. The strength of your system depends on most of the same manual procedures and controls that exist today. But, password security and two-party authorization of transactions are also required. And, the wire activity report and bank confirmation documents must be agreed to the total of all individual electronic documents processed during the business day by an independent party.

Fraud schemes employed by fraud perpetrators involve the unauthorized use of this vital banking system to divert funds to personal use (usually a "smash and grab" event) by sending vast sums of money from U.S. banks to overseas banks. When these frauds are detected, managers often find that the following internal control weaknesses: (a) password systems have been compromised; (b) the requirement for dual authorization of transactions has been neutralized; (c) non-repetitive bank numbers have been improperly used; (d) exception reports are not prepared or monitored in this critical function; and, (e) suspense accounts are not promptly reconciled.

EFT transactions are processed over telephone transmission lines by voice, computer, and by facsimile machine. The internal control procedures associated with one of these telephone systems is described below.

The EFT computer software system belongs to the bank responsible for the entity's main depository bank account. Access to this system is by modem using a personal computer, or by public telephone. The internal control procedures are as follows:

1. Personal Computer Log-On. The Investment Officer or other designated employees turn on their personal computer and enter the software access code for the program which allows them to contact the bank to use the system for EFT's as well as other types of bank transactions. Everyone in the office uses this one code when using the system (generic).

2. Office Password. This password identifies the user to the bank. There are two passwords used in the bank's system, each of which has 6 digits. This is a proper length of passwords for computer systems (i.e.; 6 or more characters, using a variable of numbers, letters, and symbols). Everyone in the office uses this one set of codes when using the system (generic).
3. Individual Password. This password permits the individual to process transactions once the wire transfer portion of the computer software system has been activated. This is a limited access program with the potential for 4 office operator identification numbers. The individual password has 6 digits.

4. Password Changes. The entity controls their own passwords; but initial passwords are established with bank assistance. These passwords can be changed on any frequency desired. However, the bank requires that passwords be changed at least every 6 months to ensure integrity within the system. The bank reportedly doesn't know these passwords, even though they are recorded in their computer. If they so desired, they could find out what any password really is. But, they advertise that this is not their intention, because it's none of their business.

5. Repetitive Bank Numbers. When the system is initially installed, the entity establishes a standard list of repetitive bank numbers for all anticipated future usage. These are established by letter from the Treasurer's Office to the bank, and are authorized by 3 signatures (i.e.; Treasurer, Investment Officer, and Fiscal Technician). All personnel indicated above are required to be signatories on the entity's main depository bank account where the EFT transactions are processed.

If additional transactions are needed for banks not listed on this pre-authorized list, additional non-repetitive bank numbers can be entered into the system. These are initiated on a one-time basis for the current date only, and must be authorized by telephone by the same 3 authorized signatories identified above.

6. Notification of Recipient. Before initiating a transaction, the Investment Officer telephones the recipient to advise them that an EFT is being sent on the current date. The recipient then monitors the EFT transaction activity in their bank account to ensure receipt of the transaction.

7. Daily Security Code. The Investment Officer devises a daily security code according to instructions received from the bank. This code must be calculated and used for each individual EFT transaction. It has 2 components as follows: (a) a code for the current date (provided on a chart by the bank); and, (b) a code which represents the sum of the digits of the amount of the transaction to be sent (whole dollars only, excluding the cents). These 2 numeric codes are added together to make the daily security code for the EFT transaction to be sent.

8. Second Person Authorization. The bank's software system for EFT transactions has an option for a second person to authorize the transaction after all the data has been entered (either at the time the transaction is entered in the system, or subsequent to this time during the same day and in a batch mode). For instance, if several people input transactions during the day, the section supervisor could review and authorize transactions processed by all office personnel at one time.

9. Dollar Limit. The bank system requires that dollar limits be established for each individual EFT transaction as well as for the total amount of all EFT transactions that can be processed by the office on a single working day.

If it becomes necessary to process EFT transactions in excess of these dollar limit amounts, exceptions can be made by placing a telephone call to the bank to bypass this control. The bank has to agree to this option, and then also becomes responsible for their action in the matter. These exceptions are initiated on a one-time basis for the current date only, and must be authorized by the same 3 authorized signatories identified above.

10. Control Log. All EFT transactions are entered in the check register for the main depository account as they occur (recorded as "EFT" rather than entering a normal check number). In addition, the Investment Officer can print a copy of each EFT transaction processed during the day, or can print a copy of a Wire Activity Report at or near the end of each operating day. The Wire Activity Report indicates the complete details of all EFT transactions, both incoming and outgoing (includes more complete data on all EFT transactions). This document or a list of the individual EFT transactions serves as a control log of all EFT transactions processed during the day.

11. Bank Confirmation. All EFT transactions are confirmed daily by the bank via mail using a Notice of Funds Transfer document. These documents are agreed to the check register entries recorded in the main depository account for all EFT transactions processed on the previous business day.

12. Reconciliation. The Wire Activity Report and bank confirmation documents are used during the daily cash balancing actions taken in conjunction with preparation of the daily cash accountability document in the treasurer's office. These documents are agreed to the total of all individual EFT transaction documents processed during the previous business day. This reconciliation is performed daily by an independent third party who does not have any responsibility for processing actual EFT transactions.

13. Daily System Report. Each morning, the Investment Officer accesses the wire transfer system at the bank and prints a System Report of all banking transactions of the previous business day. This report provides a daily record of all EFT transactions (at the summary level only for both incoming and outgoing transactions) that were processed by the treasurer's office. It also presents a daily history of all recorded transactions in the main depository bank account on the previous business day. This document is primarily used to reconcile total checking account activity during the previous day. It is used by several personnel in the office, and is in addition to the Wire Activity Report which is specifically used for EFT transaction history data during the daily cash balancing actions taken in conjunction with preparation of the daily cash accountability document in the treasurer's office. Both reports indicate EFT transaction history data, but the Wire Activity Report is filed with the daily cash accountability document. The Daily System Report is filed separately in the warrant redemption section of the treasurer's office.

The entity can also access the bank's computer software system and inquiry the wire transfer portion of the system to determine what EFT transactions have been recorded in the system at any point in time during the current working day. They can obtain a list of all incoming EFT transactions, all outgoing EFT transactions, or both. If the entity was waiting for an incoming EFT transaction and wanted to know if it had been received by the bank, they would use this program option to obtain the needed information. Thus, the bank's computer software system has an important real-time capability.

14. Transmission Security. All EFT transactions are sent from the entity to the bank over normal telephone transmission lines. The bank's computer software system does not require data transmission scrambling. Therefore, there is no communications security consideration given in the system. And, the entity cannot change this.

The case of the incoming bank teletype message. If you're in the banking business and believe that fraud only happens to others, the information below is for you. If the following message arrived at your bank tomorrow, there would probably be an unprecedented wave of panic, dismay, and alarm. The message reads as follows:

FROM: ANOTHER BANK TO: YOUR BANK

MR. SMITH LEFT YOUR BANK IN 1989 TO JOIN US AS A SENIOR PROGRAMMER. YOU WILL RECALL YOU GAVE HIM AN EXCELLENT REFERENCE. YOU WILL THEREFORE BE SURPRISED TO HEAR THAT MR. SMITH WAS ARRESTED LAST WEEK FOR DEFRAUDING OUR BANK OF $5 MILLION. DURING INTERVIEWS HE ADMITTED USING THE SOFTWARE UTILITY "DOTTO" TO CHANGE THE BALANCES ON FILES AND TO DIVERT

AND ROLL OVER PAYMENT INSTRUCTIONS. HE ALSO SAID THAT HE USED THE SAME METHOD OF FRAUD AT YOUR BANK AND GOT AWAY WITH AT LEAST $2 MILLION. HE HAS REFUSED TO ELABORATE FURTHER. WE THOUGHT YOU WOULD LIKE TO KNOW.

BEST REGARDS, JOHN JONES, DIRECTOR OF AUDIT.

The immediate questions which arise are: (a) Could you reconstruct the programs Mr. Smith had access to and worked on while employed at the bank? (b) Could you trace what concealment activities there might have been? (c) Could you develop evidence to prove or disprove this confession? (d) What would you say to the board of directors, shareholders, and investors? and, (e) What security improvements would you put in place immediately?

Real life situations like this occur every day in the business world. Like many other frauds, this may have happened only to other banks. But, this could just as easily happen at your firm. It's surprising how people's attitudes change after an event such as this happens to them or to their company.

The Federal Bureau of Investigation issued the following statistics which show how money changes hands in the U.S. These statistics give you some interesting facts about how entities conduct business. They also indicate where the risk lies within the cash handling function.

	Transaction	
Category	Number	Dollars
Cash	80%	5%
Check	18%	12%
EFT	2%	83%

Auditors primarily work with the cash and check categories during routine engagements (i.e.; 98% of the transactions and 17% of the dollars). But, the high risk lies in the EFT category. In order of frequency, these represent transactions for investments, payroll, and other miscellaneous payments.

> Investments. Since almost all transactions are conducted between the entity and pre-authorized repetitive bank numbers, these transactions are quite routine and probably represent the least risk for manipulation. Collusion would be required to manipulate these funds after they were received at the destination bank. This is particularly true in governmental entities because funds cannot be diverted out of the investment system (i.e.; all outgoing transactions are destined for authorized banks to purchase investment instruments, and all incoming transactions are destined for the entity's main depository bank account). Unlike commercial banks, employees of governmental entities do not, and can not, establish an "account" to receive the proceeds of any illegitimate transfer. This is the best possible safeguard against unauthorized EFT transactions in the investment system. Conversely, transactions between the entity and non-repetitive bank

numbers are the highest risk because fraud perpetrators would most likely use this method to abuse the system.

Payroll. Similar to the investment system, the payroll system is also a low risk environment. The critical controls in this system involve the transfer of funds from the entity's bank to the bank processing the EFT payroll transactions. The primary risk is not that an improper funds transfer will occur on this massive payroll transaction for the entity as a whole, but that unauthorized (ghost) employees names will be included on the payroll list. And, this scheme will be perpetrated within the entity. Refer to the section on payroll schemes for additional information.

Other Miscellaneous Payments. Since these transactions will most likely be destined for non-repetitive bank numbers, they are automatically high risk. Since fraud perpetrators would most likely use this method to abuse the system, these transactions require the most scrutiny.

Red Flags:

Inappropriate access to the wire room or EFT transaction processing area (i.e.; unrestricted access, or too many people).

Wire room or EFT voice or computer passwords are not changed periodically or when individuals terminate employment.

EFT voice or computer passwords are written down somewhere in the office.

Dual authorizations to process EFT transactions are either not required or are optional.
The entity or bank does not use call-back procedures to ensure that all transactions are properly authorized and approved, or the same person receiving the request performs the call-back duties.

Dollar limits for individual EFT transactions or for the entire EFT processing department are not established or are not monitored to ensure that processing is conducted only within established limits.

Exception reports listing EFT transactions are either not prepared or are not monitored daily.

Control logs are not established for EFT transactions processed each day.

EFT transactions to non-repetitive bank numbers are not specifically reviewed by supervisors for propriety.

Bank and entity reports of EFT activity are not reconciled daily.

EFT transaction suspense accounts are not promptly reconciled.

Bank wire room transactions are not encrypted during transmission.

New employees work in the wire room or EFT processing department.

Background checks are not made on all employees working in the wire room or EFT processing department.

The wire room or EFT processing department does not tape record all transactions.

Fraud Detection:

Be observant of activities at all wire rooms and EFT transaction processing areas, and determine whether access to the wire room or EFT transaction processing area is appropriately restricted.

Determine whether managers require that EFT voice or computer passwords be changed periodically or when individuals terminate employment, and whether employees write them down somewhere in the office.

Evaluate key controls for the wire room and EFT transmission area to determine whether: dual authorizations are required to process transactions; dollar limits have been established for individual transactions and daily department totals; exception reports are prepared and monitored daily; control logs are established; and, bank and entity reports of EFT activity are reconciled daily.

Determine whether the entity or bank uses appropriate call-back procedures to ensure that all transactions are properly authorized and approved.

Determine whether EFT transactions to non-repetitive bank numbers are promptly reviewed by supervisors.

Determine whether EFT transaction suspense accounts are promptly reconciled.

Determine whether bank wire room transactions are encrypted during transmission.

Determine whether the wire room or EFT processing department tape records all transactions.

CASE EXAMPLES

A market coordinator for a Mid-West oil company stole $473,541 by processing two EFT transactions in the company's oil margin accounts in an 11 month period. These transactions transferred funds from the company's margin account (managed by a broker in New York) to her husband's failing business, a non-alcoholic dance club for teenagers, in San Antonio, Texas. These funds were then diverted to other bank accounts to conceal and disguise the nature and source of the money. The couple also bought 3 cars for cash. Segregation of duties was the major cause of this loss. But, this was compounded by a lack of reconciliation of cash transactions in the margin account and a lack of independent authorization of any unusual account transactions. No one had access to the margin accounts except the market coordinator, and no one independent of the function reconciled the accounts. Finally, the broker handling the margin account had never received a list of the authorized bank accounts for routine transfers from the account, and did not use call-back procedures to verify transactions. The market coordinator managed 6 margin accounts, and informed the broker that the dance club was a company subsidiary. While there were 32 missing account statements and 13 xerox account statements in the company's files, a thorough investigation proved the existence of only 2 irregular EFT transactions in 1 margin account. The documents associated with these two transactions were falsified, and margin account statements were altered in an attempt to conceal the loss. Letters of authorization for the fraudulent EFT transactions were sent from the company to the margin account broker by facsimile machine. These letters (source documents) represented a "cut and paste" effort by the market coordinator to obtain the signatures of other company officials needed to authorize and approve the transactions. The first fictitious transaction occurred 2 weeks after the margin account was opened. An audit found the margin accounts in disarray (by design), and recommended that they be independently reconciled by the accounting department. After being pressured by the accounting department, the market coordinator resigned. Subsequent reconciliation of the accounts revealed the 2 irregular EFT transactions. There were 2 counts each of mail and wire fraud for the two facsimile and EFT transactions involved in this case. The market coordinator promptly confessed and was sentenced to 5 years in prison, five years probation, and full restitution. Her husband pled innocent to all charges in the case, stating that he thought the money came from his wife's family inheritance. The funds manipulation between bank accounts and the fact that no one else in the family was told of the inheritance led to his conviction. He had no credibility with the jury, and was sentenced to four years in prison.

A bank employee perpetrated a $10.2 million fraud through the EFT system of a major U.S. bank. The employee found the telephone access number of the wire transfer room on the wall while he was developing a back-up EFT system for the bank. He then went to a pay phone, called the wire room identifying himself as a bank employee of the international department, and transferred $10.2 million to a bank account in New York. These funds were then transferred to Zurich, Switzerland, where the individual enlisted the aid of another bank employee in the purchase of diamonds for resale. The individual then transported these diamonds through customs and back into the U.S. The fraud was detected when the individual discussed the matter with some friends and an attorney who all turned him in to the Federal Bureau of Investigation. There were weaknesses in the bank's computerized EFT system, with unreconciled transactions in the bank's suspense account for over 6 months without resolution. The bank assumed there was a computer problem in the system (fatal flaw).

A supervisor in the wire room, in collusion with 6 co-conspirators, stole $68.7 million from a major U.S. bank in the Mid-West. The caper took 1 month to plan and 1 hour to execute. Aided by a gang of accomplices outside the bank and his knowledge of a few secret codes, this trusted bank employee executed EFT transactions transferring money from accounts belonging to major U.S. corporations to bank accounts that some of the co-conspirators had set up under assumed names at 2 banks in Vienna, Austria. But, before the perpetrators could collect the loot, the bank discovered the fraud and put a stop payment on all EFT transactions. The embezzlers came tantalizingly close to succeeding and showed how vulnerable banks and their vast computerized cash movement networks can be to a dishonest insider. The supervisor of the wire room worked at the bank for 8 years before this event occurred, and had no prior criminal record or employment problems. When corporations transfer funds from their account, they contact the wire room by telephone. The bank initiates a predetermined call-back system (using various code numbers) to a designated executive at the company to verify authorization for the transaction. All calls are automatically taped. The wire room supervisor had access to the codes and knew the names of the appropriate executives at the various corporations used in this scheme. The gang originally planned to steal $232 million from the accounts of quite a few companies. However, they never got that far. On the appointed day (Friday the 13th of May 1988), the scheme was initiated. The co-conspirators of the wire room supervisor called other employees at the wire room to request that EFT transactions be processed from the target corporations to the designated fraudulent bank accounts. These transactions were then processed to the supervisor who was responsible for the bank's call-back procedures. Instead of calling the corporations indicated, the supervisor called his co-conspirators outside the bank at predetermined telephone numbers. These individuals then pretended to make the telephone conversations sound like they were real EFT confirmations. Once approvals for these transactions were falsely obtained, the transfers were initiated. The scheme collapsed (fatal flaw) when one of the corporations being used in the scheme did not have sufficient funds in their bank account to cover the EFT transaction (it bounced just like a non-sufficient funds check). All identified irregular EFT transactions were then reversed by the bank, and the perpetrators received no proceeds from the scheme.

UNMONITORED PERSONAL SERVICE CONTRACT SCHEMES

Personal service contractors (outsiders) often bill entities for services rendered in amounts greater than the amount due under the terms of the agreement. The entity must monitor these contracts to ensure that all payments are made on a reasonable time schedule, and that total payments made do not exceed the amount authorized in the contract. This monitoring can be as simple as maintaining a manual file in the accounts payable function which includes a copy of the personal services contract and a control log of all payments made to date (i.e.; total amount authorized; a schedule of all payments made by check number, date, and amount; and, the balance due).

Red Flags:

The entity does not formally monitor payments made on personal services contracts.

Personal service contract payments exceed the amount specified in the agreement.

Personal service contract payments at the beginning of the service period are excessive.

Fraud Detection:

Review the entity's monitoring program for personal service contracts for propriety.

Analyze the schedule of contract payments for unusual payments and other irregularities.

CASE EXAMPLE

The director of a county alcohol rehabilitation program stole $102,000 by processing monthly requests for payment against a personal services contract. There were no supporting documents with these requests other than an invoice which indicated "for services rendered". While the county contracted for this service at $35,000 per year for two years, they failed to monitor contract draw-downs and overpaid the contractor. In addition, the county paid the contractor an unreasonable amount of money on the first payment of each contract year. While the contract was for services rendered over a 12-month period, the county paid over 50% of the contract amount in the first payment of each year. The contractor also borrowed money from a local bank and offered the contract as collateral for a personal loan. When the bank loan officer contacted the county commissioners about the contract, they guaranteed that it was good. However, the net contract value at that time was zero because it had already been overdrawn for the period (no verification made). The county also paid off this personal loan when the director defaulted on the account. The county also established an internal auditor position after this fraud case was detected.

EMPLOYEES MANIPULATE, MISUSE, OR ABUSE MISCELLANEOUS ENTITY DISBURSEMENTS

Assets And Personnel. These abuses of power by employees are often not properly dealt with by the entity until some other major event associated with the manager is addressed. These include: (a) use of supplies, equipment, and the time of maintenance personnel for private benefit (three cases at $1,600, $1,000, and $400); (b) use of the computer to run accounting applications for a private employee business (one case at $1,400); (c) obtaining free computer disks from the manufacturer in the name of the entity and then selling them (one case at $3,200); and, (d) use of office personnel during normal duty

hours to work on projects of a personal nature (one case at $1,000). Criminal intent is difficult to prove in many cases (civil restitution only).

Credit cards. Employees use entity charge cards to purchase items for personal use from vendors. This same thing happens when the entity has an open charge account at office supply stores and maintenance supply houses. Bills are paid through the accounts payable system without questioning the purpose of the purchase or who was responsible for the transaction, and what happened to the assets.

Telephone. Employees easily abuse entity telephone systems for personal gain (two cases of long-distance telephone abuse at $1,100 and $400). Entities must establish a policy concerning the use of these systems by employees, and monitor telephone bills to ensure that personal long-distance telephone calls are not made, or are properly reimbursed by employees when these calls have been authorized. Minor abuses of the system should be dealt with through restitution and personnel disciplinary actions, while deliberate abuses should be prosecuted.

Travel. The estimated amount of expense account and travel fraud in the U.S. is $40 billion annually. While employees may abuse entity policies to obtain reimbursements for which they are not entitled, fraudulent travel expenses are usually the greatest area of concern. This includes requests for travel which the individual did not perform, requests for unauthorized travel or personal expense items during periods of official travel, and dual reimbursement of travel expenses from more than one entity. Since credit cards are often used to conceal these activities, entities must require that original supporting documents for charge transactions be included with the individual's travel voucher. Individual credit card slips and monthly credit card company billing statements are not sufficient evidence to support the reimbursement of expenses associated with most of these transactions. While this may not always be possible, such as in the case of restaurant charges, other vendor invoices and cash register tapes must be obtained by travelers when they are issued and available. Entities should also consider the amount of time required to review and audit travel expenditures when establishing employee reimbursement policies. For example, reimbursement of meals on a per diem basis rather than on an actual expense basis is not only easier and more economical to administer and audit, but also improves employee morale. If an employee is entitled to payment for a meal while in a travel status, they should receive a standard amount for each of the three meals during the day. If they exceed the authorized allowance, it's automatically a personal expense. And, if they choose to spend less than the authorized allowance, they have additional funds to spend on those items which the entity can not or will not reimburse (i.e.; laundry, gum, newspapers, toiletry items, etc.). Using actual expense reimbursement procedures for meals encourages employees to cheat on their travel vouchers in order to conceal the costs associated with many of these items. If an individual travels on behalf of two or more organizations on one trip, one travel voucher should be prepared for the individual's total travel expenses. The travel voucher should be accompanied by an explanation describing which expenses are applicable to each organization. As a result, each organization is then able to properly evaluate the claim and determine whether expenses applicable to them were authorized and for legitimate purposes. In addition, all travel voucher documents should include a certification similar to the following: "I certify under penalty of perjury that this is a true and correct claim

for necessary expenses incurred by me and that no payment has been received by me on account thereof."

INTERNAL CONTROLS FOR TRAVEL

Statistics.

Fraud in the United States amounts to more than **$400 billion annually**. Of that, the estimated amount of expense account and travel fraud in the United States is **$40 billion annually (10%)**. Travel expenses are high risk transactions because of the potential for employee manipulations regarding the events and supporting documents submitted for reimbursement purposes.

Actual Expenses Versus Per Diem Reimbursement Systems.

Entities should consider the amount of time required to review and audit travel expenditures when establishing employee travel reimbursement policies. For example, reimbursement of meals on a per diem basis rather than on an actual expense basis is not only easier and more economical to administer and audit, but also improves employee morale. If an employee is entitled to payment for a meal while in a travel status, they should receive a standard amount for each of the three meals during the day. If they exceed the authorized allowance, it's automatically a personal expense. And, if they choose to spend less than the authorized allowance, they have additional funds to spend on those items which the entity can not or will not reimburse (i.e.; laundry, gum, newspapers, toiletry items, etc.). Using actual expense procedures for meals encourages employees to cheat in order to conceal the costs of these items on their travel vouchers. Adopting the federal per diem rate system is recommended.

Travel For Multiple Organizations Or Purposes.

If an individual travels on behalf of two or more organizations on a trip, one travel voucher should be prepared for the individual's total travel expenses. Original supporting documents should be filed with the host entity. The travel voucher should be accompanied by an explanation describing which expenses are applicable to each organization. Each entity is then able to properly evaluate the claim and determine whether expenses applicable to them were authorized and for legitimate purposes. When separate travel vouchers are prepared for each organization, copies of supporting documents (not originals) are often used to commit fraud.

The traveler should also prepare separate computations for any personal travel or personal use of rental cars while in an official travel status. This document should accompany the official travel voucher filed with the entity.

Supporting Documents.

Appropriate supporting documents should be obtained by the traveler and filed with travel vouchers. Original source documents are required (no copies, with few rare exceptions). Since credit cards are often used to conceal fraudulent activity, entities must require that original supporting documents for charge transactions be included with the individual's travel voucher. Individual credit card slips and monthly credit card company billing statements are not sufficient evidence to support expense reimbursements since they are not the original source document for the transactions involved. While this may not always be possible, such as in the case of restaurant charges, other vendor invoices and cash register tapes must be obtained by travelers when they are issued and available.

Conferences And Direct Billings.

Conference brochures must be filed with the individual's travel voucher to ensure that meals and lodging provided at the event are not claimed for reimbursement by the traveler.

If the entity allows hotels and other vendors to direct bill for employee expenses, procedures must be established to ensure these direct billings are compared to employee travel vouchers to preclude the payment of duplicate expenses.

Vicinity Travel Mileage.

Vicinity travel mileage must be reasonable. Entities must compare vicinity mileage claims to other employee travel vouchers filed for specific travel events to ensure that no duplications or other irregularities occur. Adopting the federal mileage reimbursement rate is recommended.

Travel Voucher Certification.

All travel voucher documents should include a certification by the travel similar to the following:

> "I certify under penalty of perjury that this is a true and correct claim for necessary expenses incurred by me and that no payment has been received by me on account thereof."

TYPICAL TRAVEL/PETTY CASH/TIME CARD FRAUD SCENARIO

Warning: Watch out for documents which serve the same purpose as blank checks.

The Fraud: Unauthorized transactions are processed on travel vouchers (as well as on petty cash documents and on time cards/sheets/lists).

Method: All fraud occurs after approval by completing the unused lines on forms.

Prevention: Eliminate the opportunity for use of blank lines on forms (crossed-out).

Internal Control: Ensure there is a straight line from source to approval to payment. All documents must proceed directly to payment after approval rather than be returned to the source where they are altered/revised/changed/falsified.

Red Flags:

> The entity does not have, or does not monitor, policies for the use of its' assets and personnel, credit cards, and telephones.
>
> Credit card purchases are paid from vendor statements.

No one monitors employee use of the entity telephone system.

The entity does not have specific travel policies and procedures, or does not adequately review travel voucher requests for reimbursement.

Official travel forms are not used, and official reimbursement rates for various travel categories have not been formally approved for use (i.e.; mileage rate for personal vehicle use, per diem rates for meal and hotel costs, etc.).

Disbursement documents are not marked “paid” after reimbursement to preclude their reuse.

Stale-dated supporting documents are present in travel voucher requests for reimbursement.

Individuals traveling on official business on behalf of two or more organizations do not file a combined travel voucher indicating total expenses and a detailed allocation of those expenses to both organizations (full disclosure).

Separate computations are not prepared for any personal side trips or personal use of rental cars while in an official travel status.

Expenses are not supported by receipts, when required or appropriate.

Expenses for meal and hotel charges are requested even though the documents supporting the request for travel approval indicate that these expenses are included in a conference fee or will be paid by another organization.

Expenses are requested and paid for items which are specifically prohibited by organizational travel policies (i.e.; alcohol, gifts, etc.).

Vendor invoices are not originals (i.e.; xerox copies).

Mode of travel selected by traveler for reimbursement purposes, while authorized, is not the most economical mode of travel for the entity.

First class fare is used for air travel.

Travel vouchers are returned to the preparer (source) after approval rather then sent directly to accounts payable for payment.

Travel expenses indicate patterns of grossly inflated receipts, erasures and other alterations on receipts and travel vouchers, sequentially numbered and duplicate receipt numbers, and other obvious irregularities in supporting documentation.

Travelers falsify the list of individuals entertained by adding names on entertainment reports to satisfy dollar limitations for meal expenses.

Traveler completes an improper conversion of airline tickets for personal gain (i.e.; traveler obtains a refund for a company-purchased airline ticket which is then replaced by the personal purchase of an airline ticket at a reduced fare amount, such as a super saver or other promotional tickets).

Traveler obtains a refund for a company-purchased airline ticket when the related travel was either not performed, or was performed by another mode of travel at a lesser cost.

Travelers report gifts, alcoholic beverages, entertainment and personal or spouse-related expenses as meal expenses.

Travelers collect stub receipts and trade them among their colleagues.

Department managers instruct subordinates not to show expense reports to their supervisors.

Fraud Detection:

Determine whether the entity has established appropriate policies for travel and the use of its' assets and personnel, credit cards, and telephones.

Review supporting documents for each category for propriety, including authority, support, accuracy, duplication, alteration, falsification, or any other related irregularity.

When irregularities in travel receipt documents are known or suspected, obtain supporting documents from credit card companies, hotels, restaurants, and other vendors to confirm the receipt numbers actually used, the amount of actual expenses incurred by the traveler, and other details associated with the travel event.

CASE EXAMPLES

Credit Cards. The business manager of a small school district and the controller of a small hospital district stole $3,700, and $2,000, respectively, by using district credit cards to make purchases for personal use. The business manager also used several other cash receipt and cash disbursement fraud schemes to embezzle a total of $19,000 from the district. The controller also failed to repay the district for $800 in payroll advances by deducting this amount from his normal payroll checks.

Telephone and Travel. The director of a state agency stole $21,800 by misusing his position for personal gain. He used the agency telephone system to make $13,000 in personal long-distance telephone calls, filed one travel voucher for $500 in meal costs which were provided to him by another organization at no cost during the period of

travel, and then filed another travel voucher for $800 in travel expenses associated with a personal trip taken in conjunction with official agency travel. In addition, the director received reimbursement for $7,100 in other questionable or unsupported travel expenses. While hotel expenses could not be paid without proper justification when the travel destination was within 50 miles of the individual's residence or duty station, written justifications for many such trips were not filed with the travel vouchers as required. There were no supporting documents for $400 in other travel expenses.

Travel. A county sheriff and a city police chief stole $1,000 each by filing fraudulent travel vouchers for expenses associated with training at the Federal Bureau of Investigation (FBI) National Academy in Quantico, Virginia. While the FBI reimbursed them for their travel expenses to and from the academy, these individuals filed duplicate travel vouchers for these same expenses with their host employer (i.e.; the county and city, respectively).

Travel. An elected official at a school district stole $4,500 by filing duplicate travel vouchers with two entities. After receipts for travel expenses of a business trip were submitted to one entity, they were then altered, duplicated, and submitted to the second entity for reimbursement of the same expenses. Claims for automobile mileage on the same business trip were also submitted to both entities. This scheme was detected when one entity questioned xerox copies of travel documents and compared all travel expenses of this individual at both entities.

Travel. Twenty-eight officials from an Eastern U.S. railroad and motor carrier company stole $43,000 over a two year period by filing fictitious travel expenses on their travel claims (padding expense accounts). The investigation centered on 100 individuals in a company that processes about 20,000 travel vouchers a month and incurs travel expenses of $18.7 million per year. The individuals were all non-union employees making over $50,000 a year in salary, and included sales representatives, district sales managers, regional managers, area vice presidents, the vice president of sales, and the executive vice president of sales. One employee charged meals to the company from a local Red Lobster restaurant where he and his family ate frequently. Another individual charged mileage to and from a local motel where he was having an affair. Another employee had blank restaurant receipts on-hand in his office and supplied them to anyone in the department who needed forms to cover expenses. When questioned by investigators about how these bogus receipt forms were obtained, this individual smiled and stated that he had spotted a glass full of receipts at a restaurant which the waitress used when customers asked her for a cash receipt. He grabbed a handful of these blank receipt forms and stated that he had found a "pot of gold". These sequentially numbered receipt forms were subsequently used by three department employees to request reimbursement for inflated meal costs on different dates and at different restaurants all over the multi-state service area of the company. The same receipt number was also used twice (duplicate reimbursement) by employees when the receipt was issued in two copies (server receipt and payment receipt copy of same document, or carbon copy of receipt document). When this meal was also charged on a credit card, sometimes even a triple reimbursement was obtained. In many instances, individuals submitted a charge receipt for a meal expense, and then submitted the receipt for that event for a meal expense on a different date and at a different place (duplicate reimbursement). Auditors confirmed

actual expenses for these travelers with credit card companies, hotels, restaurants, and other vendors to document these travel abuses. These confirmations revealed many altered documents and inflated meal expenses. Duplicate copies of receipts (i.e.; carbon, etc.) were altered by changing either the document number or the amount. Amounts were altered as follows: (a) ones were changed to fours and sevens; and, (b) numbers were added in front of existing amounts (i.e.; $43.50 was changed to $143.50). In many instances, the type of receipt form submitted by travelers differed from the receipt form actually issued by the vendor (i.e.; type, logo, etc.). Some confirmations revealed differences even for the particular meal of the day (i.e.; restaurant charge indicates a breakfast meal, but the traveler submitted the receipt for that meal as a dinner meal at an inflated amount). Vendor receipts were also altered by cutting off the name or logo from the document to conceal irregularities. Travelers charged the company for the normal coach fare for airline travel, obtained a refund on the ticket, purchased a different excursion or super saver ticket for the trip, and then kept the difference. Travelers also charged the company for the normal coach fare for airline travel, obtained a refund on the ticket, and then did not perform the travel indicated. This company did not prosecute any of the employees cited in this case (bad judgment). Fourteen individuals resigned from the company. Thirteen individuals were returned to their original positions because management felt that resignation or dismissal would adversely affect sales and customer relations. These individuals were given official reprimands indicating that any future incident would result in dismissal. One person was refused reinstatement because of a previous travel abuse problem with the company. The results of this case sent a bad message to other company employees (i.e.; nothing bad will happen to you if you cheat on your travel voucher and subsequently get caught).

TRAVEL FRAUD CASES

January 1, 1987 Through August 31, 1998

AMOUNT	DESCRIPTION
$ 974	Sheriff was paid twice for travel to attend a federal training academy, once by the FBI and again by the entity.
28	Program director wrote checks to self for fictitious travel expenses.
184	Sheriff was paid twice for travel to attend a state training academy, once by the State of Washington and once by the entity.
8,730	Agency director filed for reimbursement of meals which were provided by the trip sponsoring organization, personal travel expenses taken in conjunction with an official trip, unsupported train and bus fares, and travel expenses for hotel and related expenses at destinations near a residence or the duty station (prohibited by agency policy).
3,034	Office assistant filed travel vouchers for vicinity travel which was not performed or which was not authorized. Supervisors signatures were

forged on documents using tracing or a rubber stamp. Fictitious travel was added to documents after approval.

425 Administrators were reimbursed for unauthorized travel-related expenses (personal telephone calls and snacks). While reimbursed for travel mileage, they also charged gasoline to the entity credit card on the trip (dual payment). The entity gasoline credit card was also used while on personal weekend trips.

2,247 Elected governing body member filed false travel vouchers with the entity and a state association seeking duplicate reimbursement from both organizations. Credit card receipts were falsified, and copies of documents (not originals) were accepted to support payments.

1,242 Elected governing body member filed false travel vouchers with the entity and a state association seeking duplicate reimbursement from both organizations. Credit card receipts were falsified, and copies of documents (not originals) were accepted to support payments.

3,004 Administrator submitted fraudulent travel claims for reimbursement. This case included the use of the same receipt multiple times, payment for meals which were provided at conferences, expenses while on personal trips, and other inappropriate travel expenses. Travel documents were also altered and falsified.

4,016 Department secretary used 391 entity taxi vouchers for personal purposes for travel to and from her residence and to other unauthorized destinations. Authorizing signature of the supervisor was forged.

3,023 Entity secretary prepared travel claims for other employees for mileage and meals even though entity vehicles were used for the travel and meals were paid by entity credit card or through direct payment to vendors. Authorizing signature of the supervisor was forged. Vicinity mileage claims were also filed even though the entity provided an official vehicle for use by the employee.

24,291 Senior marketing director filed claims under the guise of promotional hosting entertainment when the true nature of the expenses were personal (clients were not present at the events). Dates on meal documents were falsified to indicate meals were taken on different dates when in fact they were all on one day. Massage therapy charges were falsified as seminar expenses.

2,825 A judge filed false travel claims for expenses of four personal trips. Expenses for air fare, lodging, and car rentals were disguised as official court business.

17,769 Director falsified payroll and travel expense records to compensate other employees for non-existent moving costs. Unallowable moving costs consisted of charges for personal automobile mileage, food, lodging expenses, and air fare.

38,352 Fiscal specialist was reimbursed for falsified travel expenses for self and others. Authorizing signatures of other employees and a supervisor were forged.

5,641 Engineer processed false travel claims for reimbursement of lodging expenses which he did not pay, but for which he also approved payment by the consultant who did pay the bills. Other false travel claims included vicinity travel on dates when he was actually on travel status in another city and for vicinity travel for trips which were not taken.

230 Instructor convinced five students to submit false travel claims for reimbursement of non-existent expenses. The funds were used to pay for funeral expenses of a former student.

3,720 Superintendent falsified supporting documents for two disbursements to have his personal vehicles repaired at entity expense, claiming the vehicles were damaged while performing official travel. These were also unauthorized expenses because the individual was reimbursed for mileage expenses for the travel (damage must be covered by personal insurance).

3,293 Community relations specialist used entity charge card to rent vehicles for personal use, and prepared travel vouchers with forged supervisory signatures to claim reimbursement for fictitious travel.

835 Two seasonal employees used entity credit cards to obtain gasoline for their own personal vehicles on 47 occasions.

4,598 Superintendent used entity credit card to purchase gasoline for personal vehicle and was then reimbursed again for mileage for travel on official business, took personal vacations at entity expense, and filed false travel vouchers which included duplicate mileage expenses which had already been reimbursed by another association (dual purpose travel event) and duplicate hotel and meal charges which had been direct billed to the entity. Credit card receipts were used for reimbursement purposes rather than the actual receipt for the transaction. In addition, entity travel policies and procedures were deficient.

1,739 Office administrator used entity credit card to rent vehicles for personal use when not in a travel status, and used an official vehicle for personal travel.

5,854 Executive director received mileage reimbursements for use of personal vehicle when an entity vehicle was actually used for the travel. A

personal vacation was taken at entity expense, some travel expenses were not supported by receipts, and the entity credit card was used for personal travel purposes.

978 Clerk/treasurer made four joint-purpose trips and filed duplicate travel expenses with the entity and an association. Copies of expense documents (not originals) were filed as support for the reimbursement, and no one reviewed these claims for propriety.

791 Elected governing body member made a joint-purpose trip and filed duplicate travel expenses with two public entities. Copies of expense documents (not originals) were filed as support for the reimbursement.

964 Managing Director filed false claims for various travel expenses including duplicate meals, false parking expenses, excessive mileage and moving expenses, and personal expenses. The employee approved their own travel voucher without review by a member of the Executive Board.

1,883 An employee falsified four travel vouchers after they were approved by a supervisory by adding fictitious travel to the forms to increase the amount of reimbursement received.

$140,670 Totals (27 Cases) -- 8% of all cases and 2% of all dollar losses

These travel losses do not represent the largest of our dollar losses. However, they do result in unwanted media coverage, as well as ruined careers of individuals in public service.

Most travel losses, as indicated by the cases above, are attributed to key employees whose travel claims may not receive the proper level of review and monitoring by the entity.

UNAUTHORIZED CONVERSION OF DUPLICATE CHECKS

Employees obtain unauthorized payments by abusing entity lost check procedures, obtaining a replacement check, and negotiating both the original and duplicate checks.

Blank (unnumbered) checks are routinely used in many entities to replace lost or destroyed documents after issue (high risk). Reasons for losses include: misplaced, inadvertently thrown away, went through the laundry, mangled by the family pet, and many others. Blank check stock is used to manually issue a duplicate check (i.e.; same number as original) to these individuals without using the normal approval process for disbursements. A better way to process this transaction is to void the original check and cross-reference it to the replacement check (new number).

Regardless of the method used to issue replacement checks, this transaction should be supported by the individual's written certification that the original check was lost. While most entities don't issue stop payment orders to their bank on lost checks, procedures must be implemented to ensure that both the original and duplicate checks are not subsequently redeemed.

Red Flags:

Monthly bank account reconciliation is not performed in a timely manner, or is not reviewed by a disinterested party.

Inappropriate storage and issue controls over prenumbered check stock.

Use of blank (unnumbered) checks.

The entity has not established procedures to govern the issuance of replacement checks.

Duplicate checks clear the bank and are unnoticed by the entity.

Fraud Detection:

Review the entity's procedures for the issuance of replacement checks.

Review certification forms for duplicate checks issued, and determine that only one of these checks has been redeemed.

CASE EXAMPLE

A county employee stole $300 by reporting that a check had been lost. The employee prepared a certification of loss form for the entity, and a replacement check (blank check with the same number) was issued. The monthly bank account reconciliation detected that the employee cashed both the original and the duplicate check. The county subsequently obtained reimbursement from the employee for this overpayment, and took appropriate personnel disciplinary action.

STEALING AND CONVERTING BLANK CHECK STOCK

Employees and other individuals steal blank checks from storage locations and cash them.

Major areas of concern associated with blank checks are storage and issue controls.

Storage. Blank check stock must be safeguarded in storage. Access to the storage location (i.e.; vault, locked storage room, etc.) must be restricted to only a few authorized personnel.

Issue. A log must be maintained to control the issue of all blank check stock (i.e.; payee name, date, amount, number assigned, purpose of issue and cross-reference information, and the name of the individual authorizing the transaction).

The entity must retain a record of the quantity of blank checks printed in the last supply order until all warrants in the series have been used (i.e.; perpetual inventory), because they can easily be used for unauthorized disbursements. These same storage and issue controls also apply to prenumbered check stock.

The entity must have procedures to process stop payment actions on any blank checks that have been reported stolen from storage.

Red Flags:

Monthly bank account reconciliation is not performed in a timely manner, or is not reviewed by a disinterested party.

Inappropriate storage and issue controls over check stock.

Use of blank (unnumbered) checks.

The entity does not retain any record of the quantity of blank checks printed in the last supply order.

Fraud Detection:

Review the entity's procedures for the storage and issue of check stock.

Review the monthly bank statements and related account reconciliations for any irregular transactions.

CASE EXAMPLES

An unknown university employee stole $10,000 by taking 4 prenumbered checks from an insecure storage area. Storage and issue controls were lax. Even though a log was maintained of all checks processed through the check signing machine, the university did not properly reconcile this log with a computer report of all checks issued to detect missing documents in a timely manner. One of these checks was negotiated on a weekend at a check cashing facility after signing it using the university's check signing machine. The individual who cashed the check used false identification which agreed with the name of the payee listed on the document. However, the check was accompanied by a university letter signed by a fictitious financial aid counselor. Prior to

cashing the check, the check cashing facility called the telephone number listed in this letter to confirm that the transaction was valid. Representing himself as the fictitious financial aid counselor, a second individual involved in this scheme then convinced the check cashing facility to process the transaction. When this irregular transaction was noted, the university notified the bank to stop payment on the remaining 3 stolen blank checks.

A temporary park service employee stole $7,000 by taking 2 prenumbered imprest fund checks from an unattended school district administrative office. When these checks were negotiated by the individual, the bank processed them normally even though this over-drafted the imprest fund. The authorizing signature on these checks was forged. The bank accepted liability for these unauthorized transactions.

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

Purchasing and Contracting Fraud Schemes

- Purchasing Schemes
  - Accounts Payable Attributes Signaling the Possibility of Wrongdoing
  - Case Study: City of Tacoma (Tacoma Dome)
  - Case Study: Clover Park Technical College
- Competitive Bid Rigging Schemes
  - Steps to Prevent Competitive Bid Rigging
- Scams, Kickbacks, and Bribery and Corruption
- Conflicts of Interest

PURCHASING AND CONTRACTING FRAUD SCHEMES

PURCHASING SCHEMES

Objective of purchasing system.

The objective of the purchasing system is to obtain the **right product** at the **right time and place**, and at the **right price**. Unfortunately, some people create fraud trying to attain this objective.

On-book purchasing frauds can be perpetrated by using either fictitious or legitimate vendors.

Fictitious Vendors. This purchasing fraud scheme involves using irregular documents (i.e.; false purchases, receiving reports, and vendor invoices), or no documents.

This fraud is perpetrated by: (a) an employee or manager acting alone; (b) a vendor or vendor employee working in collusion with an employee (this person receives and endorses the check proceeds of the scheme); or, (c) a vendor acting alone who merely submits bogus invoices for undelivered goods and/or services.

The objective of a purchasing fraud involving fictitious vendors is to obtain a check which is then converted to cash for personal gain.

Legitimate Vendors. This purchasing fraud scheme involves the use of too many documents, too many assets, or both. The irregular documents associated with this scheme are representations of false procurement activity. Conditions encountered include: (a) multiple invoices for delivery of the same item (usually partial deliveries which are high risk transactions); (b) duplicate documents or duplicate shipments of goods; (c) inflated shipping quantities for goods actually ordered (unwanted or unneeded products); or, (d) inflated quantities on receiving reports (when the products were never actually received).

This fraud is perpetrated by one of the following: (a) an employee or manager acting alone; (b) a vendor or vendor employee acting alone; or, (c) a vendor or vendor employee working in collusion with an employee.

The objective of a purchasing fraud involving legitimate vendors is: (a) to steal the excess assets obtained from the scheme, and to sell them for cash; (b) to obtain a refund check from the vendor for the excess assets (or excess documents for these assets) which is then converted to cash; or, (c) to obtain a kickback, bribe, or gift from the vendor for favorable treatment after receiving inferior quality products or excessive quantities of unneeded products.

Symptoms of these fraud schemes appear in: (a) vendor and employee files; (b) vendor account history files; and, (c) disbursement document files.

Red Flags:

Vendor And Employee Files:

Multiple vendors with the same mailing address.

Vendor who is not listed in the telephone book.

Vendor whose only address is a post office box.

Vendor whose name is only initials (i.e.; IBM or UPS).

Employee address or telephone number is the same as a vendor.

Vendor Account History File:

New account opened for previous employer of recently hired purchasing function employee.

Old account closed for new employer of ex-employee in the purchasing function.

Accounting transactions involving vendor accounts for credit entries for other than purchases, and for debit entries for other than cash (i.e.; accounting entry exceptions for normal purchases).

Any vendor account with a debit balance (i.e.; normally a zero or credit balance).

Disbursement Document File:

Disbursement transactions with inadequate or no supporting documentation.

Checks issued to out-of-town vendors have been cashed locally.

Vendors whose invoices indicate only a post office box address, or no telephone number, or both.

Inspectors determine that the quality of a substitute product actually delivered is not the same as the product initially ordered (i.e.; quality variance).

The price of the product actually delivered is not the same as that ordered from a catalog or by contract (i.e.; price variance).

Shipping reports of returned goods (either quality or quantity rejects) do not agree with vendor refund or credit records (i.e.; employees intercept refund checks from these returns and cash them).

Contract change orders list products or services which were included in the original contract (i.e.; dual payment).

Competitive quotes are not obtained on all large dollar purchases.

Prenumbered documents are not used (i.e.; requisitions, purchase orders, receiving reports, etc.).

Vendor invoices and other available disbursement documents have any of the following attributes:

Partial deliveries with no receiving report or no delivery destination.

Inspection section indicates deviations from specifications on delivered materials.

Delivery locations other than the entity's customary delivery destination. These transactions are always questionable because they may represent evidence of asset diversions (high risk).

Sequentially numbered invoices from the same vendor.

Alterations of data elements on documents (i.e.; number, date, quantity, or amount, etc.).

No product descriptions are shown on documents (i.e.; codes only).

Document is not an original copy (i.e.; xerox copy).

Vendor invoice not on company letterhead or other pre-printed form.

Unfolded (unmailed) documents, or dirty and wrinkled documents (well traveled).

Fraud Detection:

Review the vendor file for: (a) multiple companies with the same address; (b) companies who are not listed in the telephone book; (c) companies with post office box mailing addresses only; and, (d) companies which have the same address or telephone number as an employee.

Review all recently opened and closed vendor accounts for problem links between the entity, it's vendors, and it's customers. Identify all accounts opened by new procurement employees for their prior employer. Identify all closed accounts which are also the new employer of ex-employees in the procurement function.

Review vendor accounts for accounting entries which are exceptions to normal purchase transactions (i.e.; credit entries for other than purchases, and debit entries for other than cash) to identify manipulations such as adjustments and transfers to suspense accounts.

Review vendor accounts for debit balances (abnormal condition).

Determine whether prenumbered requisitions, purchase orders, and receiving reports are used by the entity.

Review the competitive bid process, including subsequent comparisons of actual purchases and prices to approved contract provisions.

Compare endorsements on redeemed checks to entries in the check register.

Review the adequacy and appropriateness of all supporting documents for disbursements, particularly purchases, including the red flags identified above.

Employees Acting Out of Character

Employees act out of character when they perform tasks outside their normally assigned job descriptions or positions. If they are trusted employees, no one within the organization questions what they do or why. When their signatures appear on purchasing documents, auditors may not realize the true identities of the persons behind the transactions. This is especially true if the signatures are not even legible.

The illustration below is a simplification of the purchasing process for training purposes. It depicts a single document with three major components: (a) A narrative description of the item being purchased; (b) The signature of the person performing the receiving function; and, (c) The signature of the person authorizing accounts payable to make the payment. Depending upon the size of the organization, there could be several documents involved. For example, there could be a requisition form, a purchase order, a receiving report, or a vendor's invoice involved in a single transaction.

Purchase Order Document (Example)

Number

Nomenclature

Narrative description of item being purchased.

(Receiving Report)	**(Approval to Pay)**
(Signature)	(Signature)
Name/Position/Date	Name/Position/Date

The purchasing internal control checklists that I have seen through the years usually ask if two individuals have signed the supporting documents: (a) The person receiving the merchandise; and, (b) The person authorizing the payment. While I followed these steps early in my career, this work is just not good enough to find fraud. We often assume that the individuals signing

these documents occupy a position in the organization that is authorized to perform these functions. Since that is not always the case, making this mistake can lead to tragic consequences. Accordingly, auditors need to look beyond the signatures on purchasing documents.

One of the key points I now emphasize in all purchasing training is that auditors must determine the true identity of the people behind the transactions. If a person does not normally perform the function indicated on the form, auditors should classify the transaction as high risk and investigate further until the appropriate manager provides a satisfactory explanation of the situation. This determination cuts right to the core of the problem when fraud is involved.

There should always be a separation of duties among those ordering merchandise, signing the receiving reports, and approving the invoices for payment. There is always a high risk of fraud when one person is able to perform too many of these purchasing tasks. When this happens, an employee is acting out of character or overstepping job boundaries. The primary reason for this is that other staff members, such as those from the central receiving function, should be performing this task. Also be suspicious if the signer approves the transaction but leaves the receiving report section blank on the form.

Employees often overstep job boundaries simply to process transactions for their own personal gain. Knowing the position and job responsibilities of the person behind the signature is critical to understanding the compromise that often eludes auditors and managers in the quest for truth.

ACCOUNTS PAYABLE ATTRIBUTES SIGNALING THE POSSIBILITY OF WRONGDOING

1. Invoice is photocopied, altered (cut and paste), not the correct receipt type, or not for a service or product being purchased at the time of the transaction.

2. Invoice numbers occur in an unbroken consecutive sequence.

3. Invoices that are produced only with a dot matrix or laser printer.

4. Invoices appear to be similar except for areas that are “whited-out”.

5. Invoice amounts are always rounded.

6. Invoice does not show a vendor’s street address, only a post office box.

7. There is no telephone number for the vendor.

8. The phone number is either a residential number or is answered only by an answering machine.

9. The amount of each invoice falls slightly below a threshold for review.

10. The company has the same address as an employee.

11. The company has the same phone number as an employee.

12. Multiple companies have the same address and phone number.

13. "Knock-off" (similar sounding) vendor names are evident.

14. Vendor is pushed or preferred by an insider for no apparent reason.

15. Vendor reputation for integrity is poor.

16. Vendor makes frequent unexplained visits to purchasing or operating personnel.

CASE EXAMPLES

A vehicle maintenance employee at a state agency stole $89,300 by using his position to purchase automobile tires which were later re-sold through a private sector sports shop to the general public. He stole 1500 tires over a 16 month period (i.e.; two sets of tires for each agency vehicle). No one noticed this extraordinary usage in a dysfunctional purchasing system where one person was responsible for both the purchasing and inventory functions. This agency maintained no tire inventory records and no vehicle jacket files. This fraud was detected by feedback from a tire vendor who complained about slow payment of invoices totaling $27,000. Subsequent investigation of tire purchases revealed that the vendor didn't even have a contract to do business with the agency. When confronted by auditors, the perpetrator stated: "You just won't believe how the people in this agency drive." He ordered additional tires that same day, and was then arrested by police who were investigating another complaint from a tire dealer near the sports shop (i.e.; no sales, just mounting tires).

A material manager at a public hospital stole $4,400 by using his position to purchase supplies and equipment which were later re-sold to physicians in the private sector. These supplies included intravenous fluids, X-ray view boxes, and sutures. This district did not maintain a supplies and equipment inventory system. The fraud was detected by the Director of Surgery during the voucher review and approval process. This individual noticed that the hospital was paying for items which he knew were not being used in their operation. There were no purchase orders for these fraudulent transactions, and hospital employee's names were forged on the receiving reports to conceal this scheme.

A purchasing manager at a city transit authority stole $14,000 by manipulating purchase transactions in an inter-state fraud case. This resulted in excessive costs for these purchases. Rather than purchase bus parts directly from the authorized source, the purchasing manager informed the legitimate vendor (Ohio) that all purchases were required to be made through a supplier in another state (California). This "dummy" company was jointly owned by the purchasing manager and his father, who split the proceeds from the extraordinary markup they added to all transactions processed in this manner. The address of this company was a children's day care center where the father worked. There was no warehouse, and the address was used

only as a drop shipment point. These irregular transactions were further concealed by routing these bus parts through a legitimate vendor (Washington) who also added a modest markup. When the purchasing manager ordered these parts, he informed the legitimate vendor of the preferred source (i.e.; the California "dummy" company). These transactions also violated the city transit authority's policy which prohibits employees from processing any transaction where a beneficial interest was involved. The purchasing manager pled guilty and made restitution through a pre-trial diversion agreement with the U.S. District Attorney's Office.

City of Tacoma (Tacoma Dome) - $491,829

Scheme. The manager of the Tacoma Dome was in a position to falsely authorize purchases, take possession of the assets, and authorize payment for these transactions by signing that the assets had been received when, in fact, the assets were kept or sold for personal gain.

a. The manager ordered and picked-up assets directly from two vendors who split purchases into smaller invoices for consumable items over a period of weeks and in the same total amount (collusion). The manager kept or sold the assets for personal gain ($336,444).

b. The manager prepared invoices which a third vendor submitted to the city for goods or services which were never received (collusion). The manager and the vendor split the proceeds of these transactions ($134,554).

c. The manager ordered many small tools and other equipment through the city's open purchase order system, picked-up these items directly from vendors, authorized the city to pay the invoices, and sold the items to pawn shops or traded them for drugs ($20,831).

d. The manager worked in collusion and partnership with one vendor, using his position to influence the competitive bid process and obtain contracts for the vendor. The manager and the vendor split the profits from the contracts (unquantified loss amount, but $199,478 in questioned costs for business conducted).

Detection. Monitoring by the Tacoma Police Department disclosed multiple sales of assets by the manager to various pawn shops (a common element for fencing activities). They put him under surveillance and arrested him after completing a pawn shop transaction on February 14, 1997. The manager confessed and was terminated on February 20, 1997. The Pierce County Prosecutor charged him with first degree theft and unlawful possession of a controlled substance.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented.

(1) The manager abused his position and authority as a key, trusted employee at the Tacoma Dome and violated the code of ethics for municipal officers. However, there was an inadequate segregation of duties for his position (lack of supervisory review or monitoring).
(2) The manager picked-up and signed for assets received directly from vendors rather than having the items delivered to the dome's central delivery destination. No one questioned why such a high level management official repeatedly performed these tasks. There was a lack of audit certification for claims from decentralized locations within the city.

Detection Steps.

(1) Perform analytical review procedures for disbursements to identify any irregular patterns, and determine the existence of assets purchased in voucher tests.

(2) Review procurement procedures, particularly in decentralized locations. Determine if assets are picked-up directly from vendors versus delivery to a central delivery destination, if inappropriate or high level management officials sign for the receipt of assets, and if the entity sends letters to vendors about its policy on gifts and other inappropriate acts.

Sentencing. The manager pleaded guilty to first degree theft on November 19, 1997. Exceptional sentencing guidelines were used. He was sentenced to 60 months (5 years) confinement in the custody of the Washington State Department of Corrections.

Clover Park Technical College -- $483,344

Scheme. The instructor benefitted personally from a college class to repair processing machinery for four years. The college paid for all parts purchases and shipping costs for machinery repaired by students while the instructor received the revenue from the operation.

(1) Purchases valued at $330,671 had no corresponding collection of revenues to account for the loss in inventory. The instructor listed work-in-progress inventory for the class at market price rather than at purchase cost. The remaining inventory on-hand was falsified and overstated by at least $89,500 (67%).

(2) Revenue from machinery repairs and sales belonging to the college was deposited in the personal bank accounts of the instructor ($145,723) and an assistant ($6,950).

The objective of the Processing Machinery Maintenance and Repair Program is to teach students to repair machinery for food processing businesses. In this program, customers supply machinery to be repaired, the instructor orders parts, students receive experience making repairs, and customers pay for parts, shipping costs, and a reasonable labor fee when the work is completed.

Detection. A routine college review of revenue, expenditures, and inventory for the program detected irregularities including expenditures which exceeded revenues, and a work-in-progress inventory which continually increased over time. Accounting records were destroyed or removed from the college campus after the instructor was confronted with these irregularities.

Internal Control Weaknesses (Red Flags). Policies and procedures were circumvented. (1) Segregation of duties problem. The instructor operated the entire machinery repair program with only minimal review or oversight. A supervisor did not periodically evaluate the reasonableness of program revenues. expenditures, or the work-in-progress inventory.

(2) The work order system was dysfunctional. Prenumbered purchase orders were not properly accounted for and controlled or cross-referenced to work orders; a work order log book was not

maintained to track work-in-progress; jobs were not properly priced; the required 50% deposit on jobs was seldom collected, cash receipts did not reconcile to completed work order sales; actual parts, materials, and supplies were not listed on work orders; work orders were not always prepared for repair jobs; and, actual job costs sometimes exceeded revenues.

(3) The instructor abused his position and authority by entering into purchasing contracts without the authority of the college, shipping parts and machinery from the college to persons and businesses without using work orders, allowing at least two out-of-state companies to use the college as their freight-on-board shipping point for sales to their own customers, allowing customers to trade parts and machinery for repair work students performed, accepting donated and traded machinery without entering it in college accounting records, and allowing individuals who had no official capacity with the college to pick-up parts from suppliers.

(4) The instructor set up a bank account and purported to be in business for himself; however, the business was not registered with the Internal Revenue Service, the Washington State Department of Licensing, the Secretary of State, or the college.

Detection Steps.

(1) Perform analytical review procedures for business-oriented classes (i.e.; machinery, automobile, electric, etc.) to determine whether revenue, expenses, net income, and inventory are reasonable and meet program expectations.

(2) Review the purchase order and work order systems for propriety and trace transactions through the system. Trace purchases to work orders, and completed work orders to cash collections. Ensure continuous movement of projects through the work-in-progress inventory account (i.e.; no unreasonable or stale-dated projects), and compliance with program policies and procedures.

Sentencing: The former employee was sentenced to 15 months in federal prison for this crime.

COMPETITIVE BID RIGGING SCHEMES

Bid rigging is any agreement or informal arrangement among competitors to restrict trade. It is an illegal act, regardless of whether this collusion is a success or a failure. Bid rigging is a violation of the Sherman Anti-Trust Act. The purpose of this act is to preserve and advance free and competitive enterprise, and encourage free and open competition.

Bid rigging is usually a product of the purchasing or contracting environment. In contracting, bids can even be rigged by employees. Bid specifications can also be tailored to favor a particular vendor. Major factors associated with this practice include: (a) just a few sources available to provide a specific product or service; (b) a lack of product substitution capabilities; and, (c) an inadequate system of internal control on the part of the purchasing or contracting entity.

There are four basic types of anti-trust violations.

(1) Bid Suppression. One or more companies who would otherwise bid on a contract refrain from doing so.

(2) Complementary Bidding. Companies submit token bids to give the appearance of competition; however, no competition in fact exists.

(3) Bid Rotation. All companies submit bids, but take turns being the low bidder on contracts.

(4) Market Division. Companies divide all available business among themselves by geographic area or by specific customers.

Bid rigging cases are hard to detect, and even harder to prove. Schemes to restrict competition are by their very nature covert (secret). Thus, the exact form and nature of these illegal activities may not always be readily visible. In fact, the activity may be elusive, even to a trained professional. A single entity may not be able to detect these schemes even when they have a large staff assigned to the purchasing or contracting function. It takes a very sophisticated review to detect this type of fraud. Such a review might even include cooperation and assistance from other governmental entities or companies which are involved in similar types of contracting with the firms involved in the bidding process. Since these investigations might extend beyond the jurisdiction of this agency, we may decide to let another state or federal organization be the lead agency on the subsequent investigation.

The state of Washington has many statutes which establish the rules and regulations which governmental entities must adhere to for competitive bids for varying purposes. This includes construction events of all types, and individual products or product lines as well. These products include such common and every day things as vehicles, computers, paper, milk, and a whole host of consumable items which also vary by the type of entity involved. In each case, specific bid laws must be reviewed to determine whether they are applicable to the contracts being audited.

Many political subdivisions have no specific statutory public bidding requirements, some entities have only limited requirements, and others have quite extensive requirements. SAO Audit Services has prepared a summary of these laws by type of political subdivision which includes the following: (a) a matrix of bid law requirements for each entity type specifically addressed in the statutes; (b) a detailed discussion of these requirements; (c) definitions of commonly used terms; and, (d) bid law compliance problems which have occurred in the past.

STEPS TO PREVENT COMPETITIVE BID RIGGING

1. Train purchasing and contracting personnel in the elements of bid rigging and how to detect it.

2. Establish incentives for purchasing and/or contracting personnel to detect and report potential instances of bid rigging.

3. Make purchasing or contracting records available to others, if needed, and review them for trends.

4. Expand the list of potential bidding companies on all types of contracts. As a general rule, receipt of five or more contract bids usually results in the low bidding company being lower than the governmental entity's estimate of the cost of the contract.

5. Consolidate purchases where practical to achieve economies of scale.

6. Keep the contract award process as confidential as possible to preclude bidding companies from knowing everything about the procedures the governmental entity uses during the bid evaluation and award process.

7. Require firms previously convicted of bid rigging activities to: (a) submit a certified public accountant review for potential anti-trust violations; and, (b) maintain a detailed log of all contacts with firms in the same industry. Better yet, avoid these firms when possible.

Red Flags:

Bidders who are qualified and capable of performing on a contract, but who fail to bid with no apparent reason. A condition where fewer competitors than normal submit bids typifies this situation which could indicate a deliberate scheme by certain companies to withhold valid bids.

Certain companies always bid against each other. Or conversely, certain companies never bid against one another.

The successful bidder repeatedly subcontracts work to companies that submitted higher bids; or to companies that picked up bid packages, and could have bid as prime contractors, but did not.

Different groups of companies appear to specialize in federal, state, or local jobs exclusively. This might indicate a market division by class of customer.

There is an apparent pattern of low bids regularly recurring. For example, one company is always the low bidder in a certain geographical area, or in a fixed rotation with other bidders.

There is an inexplicably large gap between the winning bid and other bids. Successful bids are significantly higher than government cost estimates or previous bids.

Failure of original bidders to re-bid (or an identical ranking of the same bidders upon re-bidding), when original bids were rejected because they were too far over the entity's estimate, or for some other valid reason.

One company appears to bid substantially higher on some bids than on other bids with no logical cost difference to account for the increase. For example, a local company bids

higher prices for an item to be delivered locally than it does for delivery of the same item to points farther away.

Companies which ship their products a short distance bid higher than those who must incur a greater expense by shipping their products long distances.

There are identical bid amounts on a contract line item by two or more companies. Some instances of identical line item bids are explainable because suppliers often quote the same prices to several bidders. However, a number of identical bids on any service-related item should be viewed very critically.

Companies frequently change prices at about the same time and to the same extent.

Joint venture bids where either partnership company could have bid individually as a prime (i.e.; company had both technical and production capability), but did not.

Any incidents suggesting direct collusion among competitors, such as the appearance of identical calculation or spelling errors in two or more competitive bids, or the submission by one company of bids for other companies.

Competitors regularly socialize or appear to hold meetings, or otherwise get together in the vicinity of purchasing and contracting offices shortly before bid filing deadlines.

Assertions by employees, former employees, or competitors that an agreement to fix bids and prices or otherwise restrain trade exists.

Bid prices appear to drop whenever a new or infrequent bidder submits a bid.

Competitors exchange any form of price information among themselves. This may result from the existence of an "industry price list" or "price agreement" to which companies refer in formulating their bids. Or, this may take other forms, such as discussions of the "right price".

Any reference by bidders to "association price schedules", "industry price schedules", "industry suggested prices", "industry-wide prices", or "market-wide prices".

A bidder's justification for a bid price or terms offered because they follow the industry or industry leader's pricing or terms. This may include a reference in the bid package that the company follows a named competitors pricing or terms.

Any statements by a representative of a company that the firm "does not sell in a particular area", or that "only a particular firm sells in that area".

Statements by a bidder that it's not their turn to receive a job. Or conversely, that it's another bidder's turn.

<u>Fraud Detection</u>:

Review the entity's competitive bidding practices and procedures. Determine whether:

Sealed-bid procedures are used. A lack of control over contract bids may result in rigged bid documents through falsification of data or "leaking" quotes of other companies to the preferred company.

Adequate records are maintained indicating the amount each contractor bid, and the justification for selecting other than the low bidding company.

There are bidders who rarely win contracts. In these instances, verify the existence of these companies to identify the possibility of a controlled group bid rigging situation.

Bid specifications are written in such a way that they are specifically tailored to favor a preferred contractor.

There is a high volume of contract change orders, change orders for unusual purposes, or change orders for work which was actually included in the original contract. In these instances, low bids may have been accepted with the understanding that change orders would be processed later to make up for the difference.

Actual costs on "cost-plus" contracts are inflated, especially when there is no published price on non-price listed items included in the contract. "Cost-plus" contracts are a high risk type of contract.

There is an unwarranted substitution of non-price listed items on construction contracts.

There is a high volume of purchases or invoices approved by entity employees which are at or near the individual's maximum approval level. This might indicate the splitting of high cost items on contracts.

All construction contracts include a standard clause granting authority for the entity to audit the contractors' records. If this clause is not present in contracts, the entity and their audit representatives have no authority to review these records.

CASE EXAMPLES

In June 1991, a case of bid rigging hit the news in the state of Washington.

As specialists in sophisticated underground construction, only four companies submitted bids to the Army Corps of Engineers to repair an earthen flood control dam near Enumclaw. These companies conspired to submit proposals that were **twice** the actual cost of the project, and then planned to share the profits among themselves. By submitting artificial and non-competitive bids that contained false and fictitious prices, this bid rigging scheme eliminated competition and restrained interstate trade and commerce. Each of these companies pled guilty to one count of violating the Sherman Anti-Trust Act. The maximum penalty for a company convicted of violating anti-trust

laws is a fine of $1 million, twice the monetary gain the company derived from the crime, or twice the monetary loss caused to the victims of the crime, whichever is the **greatest**.

Three of these companies agreed to let the fourth company submit the low bid to build a concrete slurry wall to stop water seepage at the dam. In return, the low bidding company agreed to make payments to the other companies for their assurances that they would submit higher bids on the job. The bids these companies submitted on this contract follow:

Description	Amount
Army Corps of Engineers Project Estimate	$20.5 Million
Company #1 Winning Low Bid (New Jersey)	$39.5 Million
Company #2 (Massachusetts)	$41.6 Million
Company #3 (Texas)	$41.8 Million
Company #4 (France)	$42.3 Million

When the government learned of these bid rigging activities through a confession by the company which won the bid, it awarded the contract to another trustworthy company in France. This fifth firm repaired the dam for $19.9 million, an amount which was about half of the original winning low bid, and just under the original Army Corps of Engineers estimate for the job. This case involved three agencies (Justice Department's Anti-Trust Division, U.S. Attorney's Office, and Defense Criminal Investigative Service), and took over three years to complete.

Prior to June 1989, three East-coast companies that performed dredging work for the Army Corps of Engineers conspired to share the total amount of available government work among themselves by geographic area. While all three companies submitted bids on all dredging projects on the east coast, the company which had its headquarters within the specific geographic region where the work was located (i.e.; northern, central, and southern United States) always submitted the low bid on contracts within that geographic region. At first glance, the bids on these contracts could have been legitimate because of the geographic location of each company. However, the government proved that these firms actually conspired among themselves to share this dredging work by geographic area.

In September 1991, a newspaper article discussed the results of a bid rigging case involving a single product line (milk). A federal investigation of bid rigging on school milk contracts in 16 states (Washington was not included) victimized school children and cost taxpayers millions of dollars.

Since the investigation began in 1988, the Justice Department has filed 40 criminal cases against some 50 dairy companies and executives. This probe included some of the nations biggest dairies. To date, 38 dairy companies and executives have entered guilty pleas, and 18 people have received prison sentences. Seven companies and executives have been acquitted to date, and charges have been dismissed against two others.

In the latest news release on this case, Pet Incorporated pled guilty to violations of the Sherman Anti-Trust Act for fixing bids on milk contracts in South Carolina.

SCAMS, KICKBACKS, AND BRIBERY AND CORRUPTION

Scams. A scam is a fraudulent business scheme or swindle. And, a swindle is to cheat or defraud someone of money or property. Scams involve all kinds of events that are too good to be true. If something is just too good to be true, it usually is. So, beware! These scams also usually involve the general public rather than governmental entities. Perpetrators convince the target individual that they are either participating in a legitimate operation, or that they need their help. In almost all cases, these individuals are told to withdraw funds from their bank accounts. Once they do this, they are soon separated from their hard-earned money. Con-artists work an area until someone complains to the police. As soon as that action results in a newspaper article on the type of scam involved, they move to another city and start the process all over again.

Kickbacks. A kickback is a payment to a person able to influence or control a source of income through a confidential arrangement or by coercion. One of the objectives of a purchasing fraud involving legitimate vendors is to obtain a kickback or gift from the vendor for some favorable treatment. This fraud is usually perpetrated by a vendor or vendor employee working in collusion with an employee.

Accepting gifts from a vendor representative is poor judgment on the part of entity employees. All large-scale kickback schemes start innocently. Once a small gift has been received, the door has been opened for future events which are bigger and potentially more dangerous. If a person accepts a small gift, they can also accept a larger gift. They say to themselves: "Since nothing happened before, why should anything happen now?" This is the rationale used by either the vendor, the employee, or both, as they continue in this business relationship over a period of years. If the employee decides that they don't like the arrangement any more, the vendor representative might even use blackmail to achieve his objective. This could be as simple as the vendor saying to the employee: "If you don't do what I ask, I'm going to inform your employer that you have already accepted gifts in the past." Thus, to avoid being exposed, and possibly loose their job with the entity, the employee decides to continue in the relationship. And, once that initial guilt barrier has been broken, a small kickback scheme will quickly progress to a large-scale operation (progression).

Bribery and Corruption. Bribery is the act or practice of giving, offering, or taking a bribe. And, a bribe is something, such as money or a favor, offered or given to someone in a position of trust to induce them to act dishonestly, or to influence or persuade them to take a particular action or point of view. Corruption is the act or result of corrupting. And, corrupt is anything dishonest, immoral, perverted, or depraved.

A vendor might make payments to an employee to gain preferential treatment. This preferential treatment could take a wide variety of forms, and the circumstances vary depending upon the nature of the business involved. Or, employees may even create a false opportunity for business. Certain activities may not even be necessary in the routine conduct of business for the company or governmental entity. Thus, all expenses for these activities are a waste of funds.

Bribes have a significant impact on overall operations, because the effect of these illegal payments is usually much greater than the benefit attained by the employee. **Typically, a $1**

bribe results in a $1,000 loss to the victim company or governmental entity. Illegal vendor payments to employees of governmental entities can take many forms.

(1) Cash or check payments. These funds are easily spent to improve the individual's life-style. But, if these funds are deposited into a personal bank account, the results of this illegal activity can be reviewed when we subpoena the individual's bank account.

(2) Gifts of all types, entertainment, and travel. These activities are more costly and more difficult to prove than cash or check payments. The source of funds used for these events must be determined. You're half-way there once you determine that the individual didn't use their own personal funds to obtain the benefit being investigated. If they didn't pay for it, the next question is: "Who did, and why?"

(3) Offers of future employment of the target employee or their relatives. This is particularly true of individuals in the various branches of the military service who plan to retire and subsequently go to work for the vendors they deal with in their current positions within purchasing or contracting functions. But, the same condition could exist for employees of any governmental entity.

(4) Free goods and services. These can be just about anything. So, let your mind do the wandering on what some of these goods and services might actually be. These activities are also very difficult to prove.

Red Flags:

Complaint received by the police that a particular scam is operating in the vicinity.

An article appears in the newspaper, or a company/entity sends correspondence to their customers, which discloses that a con-artist is perpetrating a particular scam in the area.

Competitive bidding is not used in the purchasing or contracting functions.

The purchasing or contracting functions favor particular vendors.

Excessive quantities of materials and supplies are either purchased or are in inventory, or both.

The quality of materials and supplies purchased is inferior, resulting in increased scrap and waste, defective merchandise, and increased costs of goods or services.

The level of merchandise returns to vendors is excessive.

The life-style of purchasing or contracting function employees changes significantly for no apparent reason.

Vendor accounts are not routinely rotated among purchasing function employees.

Expenses are incurred for purposes which do not appear to be necessary in the conduct of business for the company or governmental entity.

Vendors routinely send small gifts to employees in the purchasing or contracting functions, either at home or the office.

Fraud Detection:

Determine whether the entity has established an employee communication system which is designed to ensure that tips concerning any irregularities (particularly those in the purchasing and contracting functions) are reported to management. This step is critical because if scams, kickbacks, and bribery and corruption are present within an entity, there are few, if any, routine audit tests that can be performed to detect them. There are no accounting records available to review when these frauds occur. The entity must receive a tip from a source, either inside or outside the organization, that something is wrong before an investigation is begun.

Determine whether competitive bidding procedures are used in the purchasing and contracting function.

Review purchases and inventories to determine whether excessive quantities of materials and supplies have been acquired.

Review dispositions of materials and supplies to identify trends involving inferior quality of products purchased.

Determine whether the level of merchandise returns to vendors is excessive.

Determine whether management has established procedures to identify any unusual life-style changes of employees in the purchasing or contracting functions.

Determine whether vendor accounts are routinely rotated among purchasing function employees.

Determine whether any expenses have been incurred for purposes which appear to be unnecessary in the conduct of business of the company or entity.

Determine whether the entity has a policy which prohibits employees from accepting gifts from vendors and suppliers, and whether the entity mails an annual holiday letter to companies discouraging these actions.

CASE EXAMPLES

Scams.

A private sector utility company received customer complaints (feedback) concerning their collection tactics. Research determined that a man and woman were acting as an independent team to defraud customers. During the day, the woman randomly contacted customers by telephone. She stated that the customer's utility payment was delinquent, and that someone would come by their residence to collect the amount of funds due. During the evening, the man would contact the customer in an attempt to obtain payment. Any funds paid to these individuals would be lost because they were not utility company employees. In a newspaper article, the company took this opportunity to tell their customers exactly what their collection procedures were for delinquent accounts. These included: (a) informing the public that they only make collections during the day, except when the customer specifically requests an evening appointment; (b) providing customers with a description of the uniforms worn by their employees; and, (c) indicating that all vehicles were clearly marked with the company logo.

In June 1991, banks, credit card companies, and law enforcement officials informed Congress that telephone fraud is a large problem that is getting more sophisticated and tougher to control. The most common telephone fraud cases involve low cost vacation packages, water purifiers, health and beauty aids, vitamins, and promotional pens. The general public is at risk for these types of scams.

> The newest and most troublesome trend in telephone fraud scams is the use of checking account debit cards by dishonest telephone marketers to empty personal and business bank accounts of all available funds. This state of the art scam relies on unsuspecting consumers who give out their checking account number over the telephone. The crook puts this information on a magnetically encoded bank deposit draft which is then routed and channeled between banks and accounts to steal funds. Even though millions of Americans believe that a withdrawal from their checking account cannot be made without their written consent, this deposit draft scam allows personal checking accounts to be tapped without the owner's permission.
>
> This same type of scam can occur in government because obtaining the entity's bank account number is all that is necessary for this deposit draft scam to work. Bank or entity employees could easily obtain this information. But, others outside the organization gain access to these account numbers by scavenging through the entity's trash. (This is also one of the easiest ways that hackers and outsiders use to gain access to entity computer systems.) If this scam was used against a governmental entity, a timely bank reconciliation would detect any irregular deductions from the entity's bank account. Another remedy is paper shredding.
>
> Listen to the advice of a wire and mail fraud expert, a convicted criminal who is now serving time in prison for his past dishonest telephone marketing activities.

> "First, don't give your credit card number (or worse still, your debit card number which allows direct withdrawals from your checking account) to a telephone salesperson making unsolicited calls."
>
> "Second, if you do, and are unhappy with the results, it's essential that you file a complaint. Complain to the company, police, postal inspectors office, and state attorney general's office. Curiously, only about one out of every 100 people who are dissatisfied with products and services ordered by telephone actually ask for their money back. I don't know why. I even sent some people their money back if they said they were going to call the attorney general or the postal inspector's office." Sometimes even the threat of an adverse action gets results in these cases.

Kickbacks.

A state agency employee involved in purchasing went on a weekend fishing trip sponsored by a vendor doing business with the agency. The vendor paid for the motel expenses of this state agency employee. When this case was detected by agency managers, it was fully investigated. Since this case was considered an isolated incident, this employee's improper conduct was handled through an appropriate personnel disciplinary action. In addition, future actions by all similar employees are being monitored more closely to ensure that this indiscretion does not occur again in the future. The agency had a personnel policy concerning the actions of its' employees.

Bribery and Corruption.

A city official was charged with bribery for allegedly shortchanging the entity on building permit fees to pay off his personal debts. Court documents accused this official of reducing building permit fees for a developer who lent him about $8,000. An investigation disclosed that the city was shorted almost $1,500 on two building permits issued to this developer. The crime of bribery carries a maximum sentence of 10 years in prison in the state of Washington.

The "Ill Wind" national corruption probe was a four-year Pentagon investigation of many defense contractors.

> In Spring 1990, the newspapers reported that a defense consultant pled guilty to charges of bribing two senior Department of Defense officials in exchange for their help in winning lucrative military contracts. During 1986 and 1987, this consultant attempted to steer a $100 million U.S. Navy contract to a pair of Israeli businessmen. If successful in this scheme, the consultant and a partner were then to share $2 million in payments from the businessmen. The consultant lavishly entertained Pentagon officials and defense contractors. This included elaborate dinners at his 17 acre estate in rural Virginia, chartered jet travel, and even steamship travel aboard the Queen Elizabeth II. He pled guilty to one count of conspiracy to defraud the United States and to commit bribery, two counts of bribery, and one count of income tax evasion. These felony charges carry potential maximum penalties of 40 years in prison and $1 million in fines.

In June 1991, a former assistant secretary of the Navy pled guilty to charges of federal conspiracy, bribery, and theft associated with a pattern of bid rigging and bribery. Outside consultants offered generous bribes, meals, first class travel, and gifts to government officials in exchange for sensitive bid information and clandestine help in winning multi-million-dollar business for their corporate employers. The former assistant secretary of the Navy admitted accepting hundreds of thousands of dollars in bribes from contractors. He faces 30 years in prison and fines totaling $750,000 for the following: (a) through a middleman who concealed the source of the payments, one company paid an inflated price for a condominium he sold; (b) another company provided thousands of dollars to help repair a home that he was trying to sell; (c) he also conspired to rig a Navy contract to benefit an Israeli company which had agreed to pay him and others a $2 million kickback on a $100 million contract; and, (d) he hid these illegal gains in bank accounts in Switzerland and the Channel Islands.

The government has obtained convictions or guilty pleas from 41 individuals and five corporations, and has collected more than $40 million in fines and penalties. Another corporation is expected to plead guilty in the near future, and has agreed to pay fines totaling nearly $190 million to settle these felony charges.

CONFLICTS OF INTEREST

A conflict of interest represents a basic conflict between the private interests and the public obligations of a person who occupies an official position in a governmental entity. Conflicts of interest fall somewhere in between on-book and off-book fraud schemes, because entity transactions must be matched with outside activities before irregularities are detected. Some of these conflicts follow:

The private interests of an elected public official may involve some type of transaction (usually a disbursement) between the entity and the individual as a private citizen. However, these private interests most often involve some type of transaction between the entity and a private business that the individual either owns or manages.

The activities of an employee may involve any of the following private interests which conflict with the interests of their employer.

An employee who has a part-time job at another private business, or who has two full-time jobs may cause undesirable employment conditions such as poor on-the-job performance or a high absentee rate. The entity may even want to take disciplinary action against this employee for these conditions.

An employee who has a part-time job at a supplier or customer of the entity may lose some independence and objectivity on transactions involving their primary employer. This relationship could result in some type of favorable treatment being provided to or on behalf of the supplier or customer.

An employee who has a part-time job with or a financial interest in a private business may result in the diversion of business to that organization. While this condition may occur in a governmental entity, it's more likely to happen in private industry.

Red Flags:

Lack of statutory report filing with the Public Disclosure Commission by elected public officials.

An elected public official who is employed by a customer, or who is employed by a vendor or contractor who does business with the entity.

An elected public official who exceeds the statutory dollar amount per month or per year for contracts or transactions with the entity.

Lack of signed reports of outside employment and annual employee conflict of interest statements.

Lack of procedures to periodically rotate purchasing officers or buyers between vendors and customers of the entity.

An entity employee who is also employed by or has a financial interest in a private business (i.e.; such as a competitor in private industry), vendor, or customer.

An employee (or close family relative of an employee) whose utility (i.e.; water, sewer, electricity, etc.) customer history file in the accounts receivable system indicates no activity, or activity resulting in unusual credit adjustments.

An employee who has no such utility accounts receivable account, but who lives within the boundaries of the service area and should have an account with the entity.

Fraud Detection.

The three step process used to determine if a conflict of interest exists follows:

(1) List the names and position titles of all elected public officials and all key appointed officials.

(2) Determine the occupation and business connections of each of these individuals by using either or both of the following methods.

(a) In a casual and discreet manner, inquire about the business and occupation of each listed individual.

(b) For elected public officials, obtain copies of the Public Disclosure Commission's records indicating employment and financial information.

For entity employees, review outside employment requests and conflict of interest statements.

(3) Identify any related party transactions, and determine whether there has been a violation of the conflict of interest or beneficial interest statutes. Sources of information include the minutes of the governing body, vendor files, vouchers for entity disbursements (i.e.; land and fixed asset purchases, construction contracts, remodeling projects, etc.), utility billing records, and rental and lease agreements of all types.

Compare entity outside employment forms to vendor or customer files to identify irregular relationships.

Compare a list of key employees to the utility accounts receivable records to ensure that all employees have accounts, and that no improper credit adjustments have been made to these accounts.

CASE EXAMPLE

The mayor of a small city was also the manager of a fruit processing plant. This plant was a customer of the city's water and sewer utility. The mayor directed the utility to charge the plant a relatively small flat-fee monthly sewer rate because he believed the city's calculated rate was excessive. When the city's rate was later proved to be accurate, the amount of lost revenue to the city from this customer was over $92,000 per year. These lower sewer bills resulted in an increased profit at the fruit processing plant, and a favorable performance record for the mayor/manager (i.e.; potential bonus). It also violated the city's sewer rate ordinance for uniform charges for services to all classes of customers. When an auditor asked the utility clerk why the plant was charged a flat-fee for these services, she indicated that this action was directed by the mayor. The auditor hired an engineering firm who independently evaluated the city's original proposed fee structure for this company and found them to be reasonable and consistent with industry standards.

FRAUD DETECTION AND DEVELOPMENT
COURSE OUTLINE

Additional Course Materials

Fraud Audit Report Findings

Cash Count Policies and Procedures
- Cash Count Policy
- The Cash Count
- Cash Count Audit Program
- Cash Count Procedures
- FYI - Staying Sharp on Cash Receipts

Risk Alerts
- County Auditor's Office
- Utility Cash Receipting Operations
- Segregation of Duties
- Check for Cash Substitution Scheme
- Checking Accounts
- Collect the Money and Steal It
- Special Funds
- Property and Evidence Rooms
- Ghost Employees
- Check/Warrant Endorsements
- Money Laundering Activities
- Utility Accounts Receivable
- Unnumbered Cash Receipt Forms
- Non-Public Fund Checking Accounts
- Bogus Checks and Check Fraud
- Destruction of Original Source Documents

Trial Preparation
- Pre-Deposition Information
- Pointers for a Witness
- Professional Standards Bulletin No. 87-4

Interviewing Fraud Suspects
- Tips on Interviewing Fraud Suspects
- Case Law Bearing on Fraud Audits
- Interview Outline Document

Fraud Audit Policy
- Policy 8110 Conducting Fraud Audits
- Policy 8120 Issuing Subpoenas and Records Seizure
  - Subpoena Forms

Fraud Audit Report Findings

BACKGROUND

February 21, 1997, we issued audit report number 57983 which covered Highline Water District operations for the period January 1, 1995, through December 31, 1995. This report included internal control weaknesses in the district's computer accounting system which are summarized as follows:

a. Unauthorized, undocumented changes can be made to the general ledger master file beginning account balances and the monthly net transaction totals.

b. Unauthorized, undocumented changes can be made to specific transaction postings to the general ledger.

c. Unauthorized, undocumented adjustments can be made to the utility billing system customer master file, changing the customer receivable balance without appearing on the customer account history. These last two functions have not been assigned any security features and can be accessed by all district staff.

Our audit also detected certain irregular cash receipting transactions which could not be resolved without extensive research of the district's accounts receivable and banking records. As a result, we began a special audit of the district's cash receipting system to address this concern. Our work confirmed that a misappropriation of public funds had occurred at the district. Accordingly, this report discloses the results of our special audit of cash receipts at Highline Water District.

SCOPE AND OPINION

This report represents the results of our audit of cash receipts at Highline Water District during the period January 1, 1995, through March 17, 1997. The purpose of our audit was to determine if cash receipts were properly accounted for and deposited in the district's bank account.

Our audit was made in accordance with generally accepted auditing standards and, accordingly, included such tests of the accounting records and such other auditing procedures as we considered necessary in the circumstances. This audit was conducted under the authority of *Revised Code of Washington (RCW) 43.09.260.*

The scope of our audit was limited to determining whether all cash receipts were properly accounted for and controlled. The scope of our work was not sufficient to enable us to express an opinion on the district's financial statements, and we do not express an opinion on the financial position or results of operations of Highline Water District.

In our opinion, as detailed in the following finding, the accounting clerk circumvented policies and procedures and misappropriated at least $298,125.73 in public funds from Highline Water District.

SCHEDULE OF FINDINGS

1. Public Funds Were Misappropriated And Accounting Records Were Falsified

Our audit of the financial records of Highline Water District revealed that at least $298,125.73 in public funds was misappropriated by the accounting clerk during the period January 1, 1995, through March 17, 1997. Accounting records were falsified in an attempt to conceal these losses. There were no federal funds involved in this case. The schedule below summarizes these losses.

Description	Amount
Accounts Receivable Lapping Scheme	$285,840.59
Unauthorized Write-Off of Customer Accounts	9,399.83
Check for Cash Substitution Scheme	2,885.31
Total Losses	$298,125.73
Less Funds Found in Employee's Work Area	(8.73)
Net Losses	$298,117.00

The following methods were used to misappropriate these funds.

a. Accounts Receivable Lapping Scheme. Funds from utility cash receipt transactions were not properly accounted for at the district. When currency payments were received from utility customers, the accounting clerk withheld the payment stubs and related cash receipts from transactions processed. Since the funds from these transactions were taken, the accounting clerk did not record these payments in the computer accounts receivable system or deposit the funds in the district's bank account. To conceal these losses, the accounting clerk then applied subsequent customer payments to the customer accounts which had been initially manipulated. The cumulative amount of the loss from payments associated with over 4,000 district customers were systematically manipulated over an undetermined period of time in this lapping scheme. However, these irregularities were not detected primarily because management did not review her work and customer feedback went directly to the accounting clerk. The amount of loss from this method was $285,840.59.

b. Unauthorized Write-Off of Customer Accounts. Without the knowledge of district managers, the accounting clerk circumvented district policies and procedures to write-off certain customer account balances which had been manipulated in this scheme. She established and used a separate

billing code for this purpose and processed unauthorized adjustments to customer accounts during the period January 1, 1995, through March 17, 1997. The amount of loss from this method was $9,399.83.

c. Check for Cash Substitution Scheme. The accounting clerk manipulated cash receipt transactions and accounting records in a check for cash substitution scheme. Check payments from miscellaneous revenue sources were forwarded to the accounting clerk for processing. Instead of depositing these funds for the purpose intended, she substituted these checks for currency from other recorded transactions on at least two occasions in December 1995 and August 1996. A corresponding amount of cash was then taken. The amount of loss from this method was $2,885.31.

During the period of this loss, the accounting clerk was responsible for essentially all functions associated with processing cash receipt transactions, preparing bank deposits and reconciling the bank account to the cash receipting journal, and posting payments and adjustments in the district computer accounts receivable system. When we discussed these irregularities with her on March 18, 1997, she confessed to misappropriating public funds from the district. Her employment was immediately terminated on that date.

The accounting clerk abused her position and authority as a valued and trusted district employee. While she had access to cash receipts, bank information, and customer accounts receivable records in the course of her normal duties, she circumvented the district's policies and procedures to perform unauthorized acts. However, the following internal control weaknesses also allowed these losses to occur and not be detected by management officials in a timely manner:

a. There was an inadequate segregation of duties. The accounting clerk received and opened mail, posted receipts in the computer accounting system, adjusted customer account balances, prepared the bank deposit, and reconciled the cash receipts journal with the bank statement. However, there was no periodic management review of the work performed by the accounting clerk which would accomplish the same objective as a segregation of duties between two or more employees.

b. The accounting clerk circumvented district policies and procedures for customer account write-offs. District policy requires all proposed write-offs to be approved by management. However, the accounting clerk created an unauthorized billing adjustment code in the billing program and wrote-off customer account balances without approval. Further, the accounting clerk directly altered customer account balances through write-offs utilizing the manual adjustment module. This module allowed the accounting clerk to override all controls and directly post adjustments to customer accounts. These deviations from district policies and procedures were not detected by management because the accounting clerk's work was not properly supervised or monitored.

c. The accounting clerk created 14 unauthorized suspense accounts in the accounts receivable system. These accounts were then used as a "plug" or "holding tank" for transaction amounts needed to reconcile the daily cash receipts journal with the daily bank deposit. These accounts were concealed from management because they were assigned numbers similar to those of other legitimate customer accounts. In addition, district managers were not aware the accounting clerk had the ability to create these bogus accounts.

d. The accounting clerk intercepted customer bills from the mail room prior to mailing, manually altered the amounts due, and then returned the bills to the mail room for distribution. Consequently, the amount paid by customers was not necessarily the amount reflected in the accounts receivable system since the amounts due had been altered after the bills were prepared by the computer. The accounting clerk also added a notice on all bills informing customers to contact her directly if they had any questions about their account. Thus, she was able to control important feedback information the district received from customer complaints about billing irregularities.

e. The accounting clerk routinely picked-up funds from transactions which were receipted over-the-counter by the cashier/receptionist. These receipts were in uncontrolled batches of transactions including both checks and currency. This gave the accounting clerk the opportunity to manipulate these transactions and perpetuate the accounts receivable lapping scheme over a long period of time without detection by management. District managers were not aware the accounting clerk actually performed this task.

f. The accounting clerk created, altered, and destroyed billing stubs received from customers with their payments to ensure the documents retained on file agreed with the amount of funds deposited in the bank. These irregular documents were not detected by management because the accounting clerk's work was not properly supervised or monitored.

We refer this matter to the King County Prosecuting Attorney for any criminal action appropriate under Title 9A RCW.

We recommend Highline Water District officials seek recovery of the misappropriated $298,117.00 and related audit/investigation costs from the accounting clerk and their insurance bonding company. We further recommend the Washington State Office of the Attorney General and the King County Prosecuting Attorney review this matter and take whatever action is deemed necessary under the circumstances. Any compromise or settlement of this claim must be approved in writing by the Attorney General and State Auditor as directed by RCW 43.09.260.

Bond coverage for all district employees is as follows:

Insurance Company:	Fidelity and Deposit Company of Maryland
Type of Policy:	Commercial Crime Policy
Policy Number:	CCP 9941578
Amount of Coverage:	$75,000 with $250 Deductible Provision
Period of Coverage:	March 26, 1996 - March 26, 1997

We also recommend district officials review overall accounting controls, correct the weaknesses outlined above, and implement an effective system of internal control designed to ensure the protection of public assets.

Auditee's Response

We agree there was a lack of supervision of the Accounting Department and there was no periodic management review of the work performed.

1. Management has taken steps to review all of the work performed by accounting personnel and to ensure that all district policies and procedures are adhered to.

2. The district has undertaken the task of reviewing with its accounting personnel recognized accounting policies and procedures which were established to prevent there being an opportunity for manipulation of accounts and theft. They will be educated in the purpose of these controls and how to recognize suspicious behavior.

3. A review of job descriptions is underway to ensure a proper division of duties among personnel, as recommended by the State Auditor, and which follows good accounting practices.

4. A new computer system has been installed which will prevent any write-offs of customer account balances or manipulation of account balances.

5. District took extraordinary steps to assist the State Auditor in uncovering the extent of the manipulation this employee did to customer accounts.

Auditor's Concluding Remarks

Based upon the response, the issues delineated in our report appear to have been addressed. We will review these areas again in our subsequent audit.

We would like to express our appreciation to staff, and acknowledge their extraordinary assistance and cooperation throughout the audit process.

Washington State University, College of Agriculture and Home Economics, Animal Sciences Department, Report No. 5820, August 22, 1997

BACKGROUND

On February 24, 1997, the Office of Internal Auditor, Washington State University (WSU), began an audit of the Animal Sciences Department, College of Agriculture and Home Economics, after cash receipting irregularities were brought to their attention by department management officials. The Department of Animal Sciences operates 11 units and accounts for numerous student clubs that process cash receipts. A student in the Cooperative Horse Organization Serving Students (C-HOSS) program gave the department two checks which had initially been made payable to the program; however, the payee on these checks had been altered to reflect the name of the department fiscal technician. These checks were subsequently deposited into the fiscal technician's personal credit union account.

The Office of Internal Auditor reviewed department cash receipting records for the C-HOSS program and interviewed the fiscal technician on February 26, 1997. During this meeting and in a subsequent meeting with department management officials, the fiscal technician admitted that she had misappropriated public funds from the department. The following morning, she gave her supervisor a handwritten slip of paper indicating that she had stolen $2,731.49 from the department and stated that she wanted to make restitution for this amount. She further stated that when funds were taken, she did not issue official prenumbered department cash receipt forms ("D" series) for the transactions and then destroyed any generic receipts which had accompanied the money.

The fiscal technician made restitution to the department for $2,731.49 and resigned her position of employment at WSU on March 3, 1997. This resignation was to be effective on the date her cumulative leave balance was exhausted.

On March 5, 1997, the Office of Internal Auditor notified the Office of State Auditor of this loss of public funds as required by state law. As a result, we immediately began an audit of cash receipts at the Animal Sciences Department, College of Agriculture and Home Economics, WSU.

SCOPE AND OPINION

This report represents the results of our audit of cash receipts at the Animal Sciences Department, College of Agriculture and Home Economics, Washington State University (WSU), during the period July 1, 1991, through February 28, 1997. The purpose of our audit was to determine if cash receipts were properly accounted for and deposited with the WSU Controller's Office cashier.

Our audit was made in accordance with generally accepted auditing standards and, accordingly, included such tests of the accounting records and such other auditing procedures as we considered necessary in the circumstances. This audit was conducted under the authority of *Revised Code of Washington (RCW) 43.09.330.*

The scope of our audit was limited to determining whether all cash receipts were properly accounted for and controlled. The scope of our work was not sufficient to enable us to express an opinion on WSU's financial statements, and we do not express an opinion on the financial position or results of operations of the Animal Sciences Department, College of Agriculture and Home Economics, WSU.

In our opinion, as detailed in the following finding, a fiscal technician misappropriated at least $44,337.75 in public funds from the Animal Sciences Department, College of Agriculture and Home Economics, WSU.

SCHEDULE OF FINDINGS

1. Public Funds Were Misappropriated And Accounting Records Were Falsified And Destroyed

Our audit of the financial records of the Animal Sciences Department, College of Agriculture and Home Economics, Washington State University (WSU), revealed that at least $44,337.75 in public funds was misappropriated by a fiscal technician during the period July 1, 1991, through February 28, 1997. Accounting records were falsified and destroyed in an attempt to conceal these losses. There were no federal funds involved in this case. The schedule below summarizes these losses.

Description	Amount
Checks payable to WSU deposited in personal credit union account of fiscal technician	$16,282.24
Check for cash substitution scheme	24,810.23
Undeposited funds from recorded transactions	3,245.28
Total losses	$44,337.75
Less restitution on March 3, 1997	(2,731.49)
Net losses	$41,606.26

The following methods were used to misappropriate these funds from revenue transactions of the Animal Sciences Department.

a. Checks payable to WSU deposited in personal credit union account of fiscal technician. Revenue checks from both recorded and unrecorded cash receipt transactions from the various department programs were taken and deposited into the fiscal technician's personal credit union account. The amount of loss from this method was $16,282.24.

b. Check for cash substitution scheme. The fiscal technician manipulated cash receipt transactions and accounting records in a check for cash substitution scheme. Check payments from the various department programs and miscellaneous revenue sources were forwarded to the fiscal technician for processing. Instead of depositing these funds with the WSU Controller's Office cashier for the purpose intended, she substituted these checks for currency from other recorded transactions. A corresponding amount of cash was then taken. The amount of loss from this method was $24,810.23.

c. Undeposited funds from recorded transactions. Cash from recorded cash receipt transactions from the various department programs was not deposited with the WSU Controller's Office cashier. The amount of loss from this method was $3,245.28.

The fiscal technician prepared duplicate Cash Deposit Reports to conceal these irregular cash receipting activities. While the mode of payment information shown on the reports turned-in to the WSU Controller's Office cashier agreed with the amount of funds actually transmitted for deposit, the mode of payment information listed on the form retained on file in the Animal Sciences Department indicated that more cash was collected than was deposited. However, the forms retained at the department had not been validated to prove that all funds collected had actually been deposited. In addition, the budget information and "D" series cash receipt form numbers listed on these forms was often reported inaccurately.

"D" series cash receipt forms were not be properly accounted for or controlled at the department or the WSU Controller's Office. Since some forms were missing or destroyed, they represent the potential for additional losses. The mode of payment was often omitted from receipts issued by the department, and the original copy of "voided" receipts was not retained on file for review.

During the period of this loss, the fiscal technician was responsible for essentially all cash receipting functions in the administration section of the Animal Sciences Department. When the WSU Office of Internal Auditor discussed several cash receipting irregularities with her on February 26, 1997, she confessed to misappropriating public funds from the department and then resigned. She subsequently declined to discuss these irregularities with us on the advice of legal counsel.

The following internal control weaknesses allowed these losses to occur and not be detected by Animal Sciences Department management officials in a timely manner:

a. There was an inadequate segregation of duties. The fiscal technician was responsible for practically all functions associated with processing cash receipt transactions and preparing Cash Deposit Reports for funds turned-in to the WSU Controller's Office cashier. However, there was no periodic management review of the work performed by the accounting clerk which would accomplish the same objective as a segregation of duties between two or more employees.

b. As described in the above finding, the fiscal technician falsified Cash Deposit Reports submitted to the WSU Controller's Office cashier and destroyed "D" series cash receipt forms. However, these irregularities were not detected by department management officials because the fiscal technician's work was not properly supervised or monitored. In addition, critical document verification steps were not taken at the WSU Controller's Office cashier function because of staff limitations. For

example, while "D" cash receipt forms were filed numerically, no one verified the accuracy of the total amount collected and recorded on the forms which were attached to and supported each Cash Deposit Report filed by the departments. In addition, no one verified that all "D" receipt forms from the departments were sequentially accounted for and controlled.

c. The fiscal technician did not make department deposits with the WSU Controller's Office cashier intact or on a timely basis.

d. The decentralized programs did not prepare daily or periodic activity reports which summarized all cash receipting activities when cash turn-ins were made with the department fiscal technician. Formal transmittal forms were not used for cash turn-ins, and funds were not immediately receipted by the department fiscal technician. In fact, program personnel often gave unaccounted for funds to the fiscal technician for further processing and deposit. These procedures represent the primary cause of all losses of funds within the department, and make it impossible for anyone to determine the full extent of losses the department sustained from unrecorded transactions. Since activity reports were not prepared for program operations, no one was able to properly monitor the accountability for funds from revenue streams within or from the decentralized programs.

e. Key transaction data elements were not monitored by the department to ensure the completeness of cash receipts turned-in by the decentralized programs. These included such things as the sequential use of prenumbered official receipt forms, occupancy reports and associated records, gross profits testing from sales of inventory items, and "Z" (total accountability) tapes from cash registers. For example, the Meat Laboratory cash register was broken for an extended period of time during the period of this loss; however, even when the cash register was operational, "Z" tapes were not submitted to the department when funds were turned-in for deposit.

f. Cash collections were not always receipted at the point of origin within the decentralized programs using official prenumbered cash receipt forms. In some instances, generic cash receipt forms were used to record these transactions; however, these forms provide no control over cash receipts because they can be obtained from any office supply store.

While the weaknesses noted above are specific to the Animal Sciences Department, College of Agriculture and Home Economics, WSU, we have reported significant weaknesses in cash receipting for the university as a whole in our prior three audit reports. WSU operates more than 150 decentralized cash receipting locations across the various campuses.

The Animal Sciences Department, College of Agriculture and Home Economics, WSU has a personnel dishonesty bond policy for all employees. However, the amount of these losses did not exceed the deductible provision of the policy.

We refer this matter to the Whitman County Prosecuting Attorney for any criminal action appropriate under Title 9A RCW.

We recommend the Animal Sciences Department, College of Agriculture and Home Economics, WSU, seek recovery of the misappropriated $41,606.26 and related audit/investigation costs from the fiscal technician. We further recommend the Washington State Office of the Attorney General review this matter and take whatever action is deemed necessary under the circumstances. Any compromise or settlement of this claim must be approved in writing by the Attorney General and State Auditor as directed by RCW 43.09.330.

We also recommend:

a. The Animal Sciences Department, College of Agriculture and Home Economics, WSU, review overall accounting controls, correct the weaknesses outlined above, and implement an effective system of internal control designed to ensure the protection of public assets.

b. WSU review cash receipting procedures in other colleges, departments, and units to ensure that internal controls over cash receipts have been properly established and are periodically monitored.

Auditee's Response

Recommendations:

a) The Animal Sciences Department, College of Agriculture and Home Economics, WSU, review overall accounting controls, correct the weaknesses outlined above, and implement an effective system for internal controls designed to ensure the protection of public assets.

University Response:

This audit, and its findings, show serious weakness in the internal control processes of the Animal Sciences Department, in the supervisory and management review of the fiscal technician handling cash transactions, and the accountability for funds in department and student programs.

The College of Agriculture and Home Economics accepts the recommendation of the audit report; CAHE has already taken steps to improve training, supervision and accountability; and CAHE will undertake additional actions, described below to "correct the weaknesses...and implement an effective system of internal control designed to insure the protection of public assets."

The actions taken and proposed to be taken are a result of audits conducted by the Office of the Internal Auditor (February 24, May 6, and June 18, 1997) and the office of the State Auditor.

I. Actions Taken by the Department of Animal Sciences:

A. Upon detection of the fraud on February 24, 1997, the following steps were immediately taken:

1. Removed cash handling duties from suspected employee.

2. Changed access to computer account files.

3. Changed department money safe combination.

4. Eliminated practice of depositing funds belonging to student clubs.

5. Began design, which since has been completed, of a spreadsheet on D-receipt information that will supplement data on revenues generated and deposited. This information will be used monthly by individual center managers and central department personnel to monitor revenue flow.

6. Purchase lockable cash bags for each unit generating income.

7. Purchased WSU-Department of Animal Sciences "for deposit only" stamps.

8. Created a cash register tape reconciliation form that is used by the Meats Laboratory to reconcile revenue processed on a weekly basis.

9. Discussed cash handling procedure with Department personnel who handle cash. Instruction was given on proper handling procedures and the need to issue a receipt for cash sales.

B. The May 20, 1997 internal audit memo addresses the fiscal management of the Meats Laboratory and cash control inadequacies and recommends a series of basic controls for the Meats Laboratory. CAHE will monitor the implementation of these procedures on a periodic basis; for example, by assigning a College fiscal review officer, to monitor the sales of meat and verify that all correct procedures are used from one hour before opening to one hour after closing sales. This review/monitoring

will continue through all areas that handle cash from the Meats Laboratory.

C. The June 18, 1997 internal audit memo recommends receipting properly for accountability at all steps when funds change hands. Implementation of this recommendation has begun, per memo form the Interim chair, June 25, 1997. CAHE monitoring on a periodic basis will verify that the correct procedures are followed.

D. Training.

1. With respect to training, CAHE held a mandatory training program, June 18, 1997, on internal controls, internal control review, and internal control review checklists. All administrative managers and fiscal technicians either attended this training, or in the case of two persons, received individualized training. The WSU Controller's Office provided the initial training to the CAHE Business and Finance Office. The business and Finance Office provided the training to the College.

II. Actions To Be Taken:

A. Training.

1. A second in-depth training program on cash receipts and cash handling is scheduled for September 23-24, 1997, at the CAHE Staff Development Workshop, Pullman. Topics include the separation of duties and accountability and compliance to the Business Policies and Procedures Manual.

2. Verification of participation will be maintained by the CAHE Business and Finance Office.

3. A special training session for all faculty and staff in the Department of Animal Sciences will address the issue of institutional business policies and procedures, the accountability for student accounts by faculty advisors, and state accounts by faculty and administrative managers.

B. Internal Accountability

1. The lack of accountability of revenue streams will be addressed by monthly review of revenues and reports to faculty advisors or managers of revenue generating programs.

2. Appropriate allocation of revenues to accounts will be monitored and verified.

3. Periodic site visits of unit programs by CAHE Business and Finance Office Representatives will verify that correct procedures are being followed.

4. Any corrective actions required will be implemented immediately

5. Responsible individuals will be evaluated based on their ability to maintain internal accountability.

C. Student Accounts

1. A recommendation of the internal auditor is for funds of student clubs to be handled through CUB accounting and the Controller's cashier. CAHE concurs.

2. When losses to specific student clubs are known, the Department will take immediate steps to reimburse the clubs for their loss with non-appropriated funds.

3. CAHE will schedule training sessions at the beginning of each school year for student club officers and faculty club advisors on cash handling and record maintenance of club activities.

Recommendations:

b) *WSU review cash receipting procedures in other colleges, departments, and units to ensure that internal controls over cash receipts have been properly established and are periodically monitored.*

University Response:

I. Actions Taken by WSU

1. The person who misappropriated funds in the Animal Sciences Department is no longer employed by the University.

2. WSU has received partial restitution of the money misappropriated and will pursue recovery of the remaining balance misappropriated.

3. The Internal Audit Office performed a cash control audit of the Meats Lab and met with the department's Administrative Manager on May 6th. A memo of May 20th details specifically how receipts should be recorded by the Meats Lab and reviewed and monitored by the Administrative Manager.

4. On June 8, 1997, the Controller's Office provided internal control training specifically to the College of Agriculture and Home Economics Administrative Managers and Fiscal Technicians.

5. The University administration had met with responsible College of Agriculture and Home Economics administrators to clearly define the problem and the requirements to resolve the issues brought forth in the various audits.

6. The Internal Auditor has directed the College to have all student organizations use the CUB Accounting Services.

II. Actions to be Taken:

1. The Controller's Office will implement a University process that will require an individual other than the one who would be issuing departmental receipts to pick-up and sign-for the official receipts from the Controller's Office.

2. The WSU Controller's Office will provide additional cash handling and internal control training to the College of Agriculture and Home Economics on September 23-24, 1997. Cash handling and internal control training will continue to be provided to all employees University-wide with cash handling responsibilities. Emphasis will be placed on those areas of concern brought forth in the audit.

3. The Internal Audit Office will perform periodic follow-up reviews within the College of Agriculture and Home Economics to ensure compliance with University policies and procedures.

4. The Internal Audit Office will place emphasis on internal controls and cash handling methods in other departmental reviews.

5. The WSU Controller's Office will assist the College of Agriculture and Home Economics Central Finance Office in establishing a cashiering operation for the College. This will allow the College to better monitor receipts and cash handling activities of the College Units to ensure compliance with University policies.

6. The Office of the Vice President of Business Affairs will develop and implement a plan to review all cash handling operations and internal control structures throughout the University to ensure compliance with established University policies and procedures. The State Auditors have offered to assist in reviewing the 150 sites. In addition, an Internal Audit position is to be added to the current audit staff to increase frequency of departmental audits and to add emphasis on cash handling and internal control policies and procedures in future internal reviews.

Auditor's Concluding Remarks

Based upon the response, the issues delineated in our report appear to have been addressed. We will review these areas again in our subsequent audit. We would like to express our appreciation to the WSU staff, and acknowledge their extraordinary assistance and cooperation throughout the audit process.

Cash Count Policies and Procedures

STATE OF WASHINGTON
State Auditor's Office NOTICE March 31, 1995
Division of Audit

TO: All State Examiners

FROM: Lee Reaves, Director
Division of Audit

SUBJECT: Cash Count Policy

Policy. State examiners in the Division of Audit will make unannounced cash counts at state agencies and local governments. Risk assessments and audit plans will determine the timing and frequency of these surprise cash counts. State examiners will use their own judgment and experience, prior audit history of the entity, and other known or relevant factors when determining the timing of cash counts. For example, this work could be accomplished at a date which is independent of the regular audit, at the beginning of an unannounced audit, or at some other designated time during the course of the audit.

The most frequent complaints raised by managers during the cash count process are that it disrupts normal business operations and detracts from the entity's ability to provide prompt customer service. These are the primary reasons some managers ask state examiners to schedule their visits or provide advance notice of the date of arrival on-site for the start of routine audits. However, concealment of fraudulent activities is another reason. Secrecy is required if these irregular practices are to continue undetected over a long period of time. Thus, advance notice assists fraud perpetrators in concealing their illegal acts.

Therefore, one of the most important things state examiners must do during unannounced cash counts is to make sure that normal business operations are not disrupted for an extended period of time. The best way to do this is to begin the cash count by verifying the accuracy of an alternate change fund. If an alternate change fund does not exist, create one. This change fund can then be used by the primary cashier or any other substitute cashier to continue normal business operations until the cash count has been completed. These actions minimize the disruption of normal business operations and help to ensure that the entity is able to provide prompt customer service even while the cash count is in progress.

The importance the agency has placed on unannounced cash counts has varied over the years. As a result, our application of cash count procedures has been inconsistent within the division. Some audit teams schedule their audits or provide advance notice of the date of arrival on-site, and do not perform surprise cash counts at any other time. Other audit teams have always performed surprise audits and surprise cash counts and have not encountered any significant problems with the process. Therefore, this policy statement is designed to remedy this situation. Full implementation of this revised cash count policy will help to ensure that all audits are consistently performed throughout the division.

STATE OF WASHINGTON
State Auditor's Office NOTICE March 31, 1995
Division of Audit

TO: All State Agencies And Local Governments

FROM: Lee Reaves, Director
Division of Audit

SUBJECT: Cash Count Policy

The importance the State Auditor's Office has placed on unannounced cash counts during routine audits has varied over the years. As a result, cash count procedures have been inconsistently applied throughout the state of Washington. This policy statement is designed to remedy this condition.

Policy. State examiners in the Division of Audit will make unannounced cash counts at state agencies and local governments. Risk assessments and audit plans will determine the timing and frequency of these surprise cash counts. State examiners will use their own judgment and experience, prior audit history of the entity, and other known or relevant factors when determining the timing of cash counts. For example, this work could be accomplished at a date which is independent of the regular audit, at the beginning of an unannounced audit, or at some other designated time during the course of the audit.

The most frequent complaints raised by managers during the cash count process are that it disrupts normal business operations and detracts from the entity's ability to provide prompt customer service. These are the primary reasons some managers ask state examiners to schedule their visits or provide advance notice of the date of arrival on-site for the start of routine audits. However, concealment of fraudulent activities is another reason. Secrecy is required if these irregular practices are to continue undetected over a long period of time. Thus, advance notice assists fraud perpetrators in concealing their illegal acts.

State examiners will ensure that normal business operations are not disrupted for an extended period of time during these unannounced cash counts. This will help to ensure that state agencies and local governments are able to provide prompt customer service even while the cash count is in progress.

Full implementation of this revised cash count policy will help to ensure that all future audits are consistently performed throughout the Division of Audit. I appreciate your patience and understanding in this important matter.

THE CASH COUNT

By: Joseph R. Dervaes, CFE, CIA
Audit Manager for Special Investigations

The cash receipting process is a high risk function in all state agencies and local governments and must be appropriately reviewed during all audits.

The Unannounced Cash Count.

There are at least four major objectives of unannounced cash counts. These are: (a) to count all funds in the custody of cashiers and managers; (b) to verify the amount of funds counted to the appropriate accountable documents and records; (c) to review and observe the system of internal control over the cash receipting process; and, (d) to review and observe the system of internal control for the security and safeguarding of cash during normal business operations and while funds are secured over-night in safes and vaults.

Unannounced cash counts can be performed in two ways:

(1) At the beginning (or end) of the business day when only the change fund is counted and agreed to the entity's record for the authorized custodian and amount.

This method does not tell you much about the entity's system of internal control over the cash receipting process.

(2) During the business day when both the change fund and all cash receipts are counted. The change fund is agreed to the entity's record for the authorized custodian and amount, while cash receipts are agreed to the appropriate accountability mechanism in use (i.e.; manual cash receipt forms issued, manual or computer cash register sub-total or "X" reading for recorded transactions, or other similar cash receipting mechanism).

This is the preferred method because it represents the auditor's only real (and best) opportunity to observe the entity's system of internal control over the cash receipting process in action. This step will confirm not only what managers have told you about their internal control procedures, but also what the employees really do through actual practice. Often, these procedures are different. Sometimes the effect of this difference represents fraud.

Internal Control Procedures.

Segregation of duties in the cash receipting function is a major area for study during all routine entity audits.

The primary issue raised by managers and auditors about segregation of duties is the number of people who should be involved in receipting, depositing, and reconciling cash receipts. The questions asked are: Should one person perform all these functions acting alone? Or, should more than one person coordinate their activities to jointly perform these functions?

The answer to these questions are not easy because it depends upon the circumstances involved. There is no one best way to perform the functions of receipting, depositing, and reconciling cash receipts. The number of people necessary to provide adequate security over cash receipts depends upon the size of the operation involved and the number of individuals employed in the activity. Thus, the internal control procedures needed over the cash receipting process vary from one entity to another. If organized properly, entity assets can be adequately safeguarded using either of the systems described below. These are: (1) one person acting alone; (2) two or more persons acting jointly; or (3) some combination of both systems. Neither system is right or wrong. Both systems are permitted.

A corollary issue is that no matter what system is used, entities must be able to fix responsibility for funds to a single individual at all times. This means there must be a policy of one cashier, one cash register, and one cash drawer. Multiple cashiers may operate from the same cash register as long as each cashier has their own separate cash drawer. This also means that all transfers of funds from one person to another during the normal business day, such as for shift changes, and at end of day must be formally documented by an exchange of receipts acknowledging responsibility for the funds.

There is no guarantee that fraud will not occur in state agencies or local governments. We've proved this year after year. A wide variety of frauds can be perpetrated by either the "doers" (the cashiers) or by the "reviewers" (the supervisors). There are too many cases of each type to ignore this fact. Both types of employees represent a risk to managers and auditors. Hopefully, the reviewers will detect fraud by the doers in it's early stages before it gets out of hand. But, who's checking of the reviewers? That's an interesting thought for you to ponder as you perform future audits. Perhaps it's you.

It's impossible to eliminate fraud completely. Therefore, it doesn't matter exactly which internal controls are in effect (i.e.; one person acting alone, or more than one person acting jointly). All fraud perpetrators simply ignore or compromise internal controls which allow them to commit the crime. These employees don't play by the rules. Therefore, management's (and audit's) response to this threat must be to periodically monitor (and audit) the system of internal control to determine if it operates as designed, and when, not if, public funds have been misappropriated. Nothing else works.

People respect what you inspect (i.e.; management review and audit), not what you expect. Therefore, periodic monitoring of the system of internal control serves as both a detection mechanism for management and a deterrent against unauthorized or irregular activity by employees. If fraud does occur, monitoring will detect it early and keep fraud losses to a minimum. That's the best that can be done.

Let's now consider the internal control procedures associated with the two employee scenarios described above.

One Person Acting Alone.

This scenario usually occurs at small entities, or at decentralized locations within large entities. In this case, a cashier works alone, and there are no supervisors present at the cash receipting location. Thus, one person receipts, deposits, and reconciles cash receipts. This is an internal control weakness that auditors must address because management review and oversight is missing. This problem can be easily remedied by having a supervisor periodically review the work of this cashier in such a way as to accomplish a segregation of duties without hiring another employee in the function. Management could accomplish this by making periodic unannounced cash counts, by verifying the check and cash composition of bank deposits, and by making other appropriate management reviews of the documents, work, and activities of the cashier.

There are two ways to make deposits under these circumstances.

(1) An individual working alone should take the daily deposit directly to the bank or to the central treasury function, as appropriate. This is the preferred method. The decentralized location cashier then turns-in their daily activity report and supporting documents to the accounting office or supervisor along with a bank validated deposit slip (duplicate) indicating the check and cash composition of the deposit.

If a commercial courier service is used to make the bank deposit, locked or tamper-proof deposit bags must be used. These often have special seals. A log record is prepared for all such transmittals which identifies the transaction by seal or bag number. The courier signs this log indicating that they have accepted custody of the deposit bag. The decentralized location cashier then turns-in their daily activity report and supporting documents to the accounting office or supervisor. The bank validated deposit slip (duplicate) indicating the check and cash composition of the deposit is returned directly to the accounting office or supervisor by the bank.

Use of the direct deposit method is not always possible, such as in certain activities at school districts. Many other entities choose not to use this method because it doesn't follow their organizational structure or meet their management or other operational needs.

(2) When direct bank deposits are not made, funds must be transmitted to the central treasury function. There are two ways to accomplish this step.

(a) Funds are hand-carried to the central treasury function by the decentralized location cashier. A two-part transmittal form is recommended for this process, although not always necessary. When used, the original of the transmittal form is given to the central treasurer, while the copy is retained at the decentralized location or turned-in to the accounting office or supervisor. When the cash turn-in is made, the deposit must be counted by the central treasurer who immediately issues an official prenumbered and controlled cash receipt form accepting accountability for the funds. (Note: If hand-carried funds are not immediately counted by the central treasurer, a transmittal system should be used to properly control these funds.) The cashier then turns-in their daily activity

report and supporting documents, including the transmittal form (if used) and cash receipt form, to the accounting office or supervisor.

Note: A cash transmittal system usually involves official prenumbered and controlled forms. Of major importance is entity monitoring of the sequential use of these forms by decentralized locations. This could be accomplished by the central treasury function, by the accounting office, or by a supervisor. Someone must know the business schedule and monitor operations to ensure that cash receipts are turned-in for each day the decentralized location is open for business. Alternative controls, in lieu of a cash transmittal system, could include such things as the date (or shift per day), "Z" tape number from manual or computer cash register systems, inventory control data, or some other numerical control which documents and proves that cash receipts were turned-in for each business day.

(b) Funds are transmitted to the central treasury function using an entity employee as a courier. Locked or tamper-proof deposit bags must be used. A log record must also be prepared and signed by the courier as described above. However, a three-part transmittal form is also recommended for this process. The original and one copy of the transmittal form accompanies the deposit, while the remaining copy is retained at the decentralized location.

The central treasurer must sign for each deposit bag received from the courier. However, these deposit bags are not always opened and counted immediately upon receipt. They are often placed in a safe or vault until a sufficient amount of time is available to accomplish this task. Two people must open and count the contents of these deposit bags. This protects both the decentralized location cashier and the employees at the central treasury function in the event of any discrepancy in the amount of funds reportedly contained in the cash transmittal. The central treasurer then issues a prenumbered and controlled cash receipt form accepting accountability for the funds. This cash receipt form and a copy of the transmittal form is then returned to the decentralized location cashier.

The decentralized location cashier then turns-in their daily activity report and supporting documents, including the cash transmittal form and cash receipt form, to the accounting office or supervisor.

Two Or More Persons Acting Jointly.

It's always desirable to segregate the duties of receipting, depositing, and reconciling cash receipts when staffing levels permit this practice. This splitting of duties and responsibilities makes good common sense, and can be accomplished in a wide variety of ways. The method selected always varies depending upon the organization and the number of employees involved. Practically any segregation of duties which prevents one employee from performing all cash receipting functions is acceptable.

One of the primary issues raised about cashier activities is how to handle end-of-shift (day) balancing. The question asked is: What is the correct way to accomplish this task? The answer is that there is no right or wrong way to do this. Two frequently used methods are as follows:

(1) Cashiers are required to count and balance their cash with accountability documents before funds are turned-in.

(2) Cashiers are not allowed to count and balance their cash with accountability documents before funds are turned-in. In this case, two supervisors must subsequently perform this step to protect both the cashier and the supervisors in the event of any controversy over the amount of funds involved.

Summary.

This document is not intended to be all inclusive. However, there is more information available on this subject in the Fraud Detection and Development training manual. Please refer to the additional material in Section 6 of the manual for a concise description of a sample cash count program and related cash count procedures. Many issues associated with access to and security of funds are also presented.

State examiners should provide advice and guidance to managers about the system of internal control over the cash receipting process. However, management must decide which system works best for their organization. In fact, both systems can be used in the same entity in different functions and under different circumstances.

CASH COUNT AUDIT PROGRAM

Review the entity's central file of authorization documents for all change and imprest fund accounts. This file should include a copy of the resolution or other approval document which established the fund, a signed receipt from the authorized fund custodian, and copies of any unannounced cash counts management officials performed on each fund.

Determine if change and imprest funds are monitored by the central focal point. Does the entity have written procedures for establishing such funds, changing the custodian or amount, and terminating the use of the fund?

Determine if the central file has been properly established and whether it is maintained currently.

Identify and list all change and imprest fund accounts in the entity, including location, custodian, amount, and purpose.

Perform an unannounced cash count of all change and imprest fund accounts.

Agree fund level to the authorized amount. Determine whether the fund level is more than, less than, or equal to the authorized amount. Obtain an explanation for any variance in the fund amount.

Determine whether the actual fund custodian agrees with the authorized fund custodian. Obtain an explanation for any changes of custodian and dates of same.

For revolving funds which are maintained in checking accounts (i.e.; purchasing or advance travel funds), obtain a cut-off bank statement as of the date of the cash count. Total cash accountability is determined by adding cash on-hand, cash in the bank, and all outstanding travel advance transactions (unsettled accounts), or unreimbursed purchases, as appropriate.

Determine if purchases are made only for authorized purposes.

Determine if travel advances are made to authorized persons for authorized purposes.

Determine if personnel settle outstanding advances in a timely manner (i.e.; within 10 days of the completion of the travel).

Ensure that all individuals settle their outstanding advance before obtaining another travel advance for a different purpose.

Perform a complete review of the internal control environment associated with the cash receipting function during your audit.

CASH COUNT PROCEDURES

Unannounced cash count (surprise) -- funds = accountability. Prepare all cash count forms in ink. Neatly make any corrections to erroneous data entries, and have the auditor and fund custodian initial them.

List next unused cash receipt form or check and take an "X" reading (sub-total) on a cash register (cut-off).

Know the change/imprest fund amount and verify to the source.

Is the custodian of the funds (actual) the same as the individual who signed for the funds?

Secure all funds and accountability documents (cease activity).

Seal safes and vaults when the fund custodian is not present.

Don't let the custodian leave you alone with the funds.

List all checks.

Agree to cash receipts (name/amount) and cross reference.

Ensure current dates (since last deposit or transmittal).

Any for custodian (loan)? or employees (cashing checks from receipts)?

Are checks restrictively endorsed "for deposit only" immediately upon receipt?

Are deposits made daily and intact?

Determine if all transactions are receipted.

Check and Cash composition of funds/deposits.

Does management periodically review this?

Are official prenumbered cash receipt forms used rather than commercially purchased or variety store cash receipt forms (i.e.; rediform, etc.)?

Is mode of payment information present on cash receipt forms and used?

Verify that the last deposit includes receipt numbers prior to the cash count for continuity of sequence.

Does management periodically review this?

Verify that all checks included in the cash count appear in the next deposit, and are not subsequently returned for non-sufficient funds (NSF).

Verify that all accounts receivable payments were properly posted to subsidiary ledger cards.

Search the cashier area for any unusual or unexpected items.

Identify any other funds on-hand (i.e.; cash over/short "slush" funds) - count and document.

Confiscate any "extra" cash receipt books.

Confiscate any "extra receipts" written over many times.

Have the fund custodian sign the cash count form acknowledging return of the funds.

Review accountability documents for the prior business day.

Is a daily activity report prepared?

Are cash receipts and "Z" tapes used sequentially?

Are they listed on the daily activity report and monitored by management?

Does the entity account for cash overages and shortages on the daily activity report and in the accounting records (i.e.; miscellaneous income and expense)?

Listen to and observe what's happening in the cash receipting area.

Do cashiers ask the customer: "Do you need a receipt?"

When was the combination last changed to any safes and vaults?

Periodic frequency (i.e.; every 6 months)?

When employees terminate employment?

Is the safe or vault combination (or computer passwords) written down by employees (where)?

How many people have access?

Is this appropriate?

Review security access to the cashier area for propriety.
What are entity procedures for voided transactions?

Supervisory approval?

Retention of all copies of voided documents?

Official “void” form used?

Review segregation of duties for personnel in the cashier function.

Is the manager’s key inserted in the cash register at all times (i.e.; “X” sub-total; and “Z” total)?

Do cashiers operate from an “open cash drawer”?

Can the entity fix responsibility for cash (i.e.; 1 cashier, 1 change fund, or 1 cash drawer, etc.)?

Does anyone monitor NSF checks and subsequent collections?

Are separate deposits made for all NSF checks?

Is a collection agency used for delinquent repayments?

Are difficult cases referred to the police for prosecution?

Are all cash receipt transactions supported by NSF check payments reversed?

Is the bonding for “employee dishonesty” adequate?

Are petty cash or other disbursement forms prenumbered?

Are the dates of all documents current (not stale-dated)?

Is the fund amount proper (i.e.; 2.5 times reimbursement cycle)?

Is the fund reimbursed frequently and at year-end?

Does the custodian use paid-out forms for cash advances?

Are all documents marked “paid” to preclude their reuse?

Are there any xerox copies of documents in the file?

Review patient or jail inmate trust funds.

Cash receipts = deposits = postings to subsidiary ledger cards.

Control account = subsidiary ledger cards (reconcile).

Cash plus bank account balance = total of all funds.

Are forms and signatures required for all withdrawals of funds (either in cash or in merchandise, such as in a commissary operation)?

FYI - STAYING SHARP ON CASH RECEIPTS

This edition of **FYI** focuses on auditing procedures commonly used when examining cash receipts. Use this to refresh your memory or to design new tests. We have provided traditional auditing procedures as well as some hints and tips lifted from the fraud detection materials prepared by Joe Dervaes, CFE, CIA. We will issue a similar **FYI** on cash disbursements soon.

INTERNAL CONTROL ANALYSIS

Here are a few questions to ask when evaluating internal controls over cash receipts. Please note that some questions may not apply to each of our auditees.

Are receipts deposited intact and on a daily basis?

Does someone other than the cashier or accounts receivable bookkeeper take the deposit to the bank? Are locked or tamper-proof bank bags used?

Is a duplicate and bank validated deposit slip showing the composition of receipts retained by someone other than the employee making up the deposit?

Do two employees open the mail and make a list of cash received (a remittance list)?

Does someone other than the cashier reconcile the remittance list to daily cash receipt transactions to ensure that all payments have been recorded properly and deposited in the bank?

Are the duties of the cashier entirely separate from record keeping for notes and accounts receivable?

Is the cashier denied access to receivables records or monthly statements?

Is a bank reconciliation performed monthly by an independent person who does not have cash custody or record keeping responsibility?

Are the cash receipts journal entries compared to the remittance lists and deposit slips regularly?

Does someone reconcile the accounts receivable subsidiary to the control account regularly (to determine whether all entries were made to customers' accounts)?

Are official prenumbered receipt books used? Do cash receipt forms indicate the mode of payment for the transaction (i.e. cash or check)? Is the numerical sequence of issuing the forms checked for missing documents?

Does the accounting manual contain instructions for classifying cash receipts?

Does the accounting manual contain instructions for dating cash receipts entries the same day as the date of receipt?

Are funds properly protected during the operating day and secured in a safe or vault overnight? Is access to the cashiering area appropriately restricted?

Is access to the safe or vault limited? Is the safe or vault combination changed periodically and when employees terminate employment? Is the safe combination written down by someone in the office?

Has the entity adopted the concept of one change fund and one cash register (or drawer) per cashier to fix responsibility for funds to a specific individual at all times?

Are checks restrictively endorsed "For Deposit Only" immediately upon receipt by cashiers?

SUBSTANTIVE AUDIT PROCEDURES

Listed below are a few suggested procedures (and the applicable financial statement assertion) to follow when auditing cash.

Existence or Occurrence

Obtain bank confirmation(s). Identify personnel who are authorized to sign checks.

Count cash on hand (petty cash and undeposited cash).

Prepare bank transfer schedule (if an entity has more than one bank).

Rights and Obligations

Review cutoff of year-end cash receipts and disbursements to ensure they are recorded in the proper period.

Review bank statement to verify that the book balance represents amount to which entity has rights.

Completeness

Review bank reconciliation to verify that cash has been properly stated at year-end.

Obtain bank cutoff statement to verify reconciling items on bank reconciliation are properly reflected.

Valuation

Foot summary schedules of cash account to see that it agrees with the total shown in the financial statements.

Reconcile summary schedules to general ledger.

Presentation and Disclosure

Review disclosures for compliance with GAAP.

Inquire about compensating balance (minimum balance) requirements and restrictions for compliance with GAAP.

Other Procedures

Determine whether cash was deposited within 24 hours of receipt. This compliance requirement is applicable to every public officer and employee per RCW 43.09.240. Note, however, that some auditees are granted a time extension by the state treasurer or a treasurer of the applicable taxing district.

FRAUDS AND FINDINGS

In reviewing fraud statistics prepared by Joe Dervaes, 73% of the statewide fraud cases from 1987 to 1994 involved cash receipts. As Joe points out, cash receipts and cash disbursements are the two major types of fraud risk. While the risk that fraud will occur in the cash receipting function is high, the dollar amount of losses from each case is small. Conversely, while the risk that fraud will occur in the cash disbursements function is low, the dollar amount of losses from each case is large.

A review of the local government findings index (available on the SAO Reference Guide) shows that 155 cash receipts findings were written from January, 1993, through April, 1996. In addition, 88 cash receipts findings have been written at the state agency level since FY90.

Below are some additional procedures and tips recommended by Joe when examining cash receipts.

Perform audit tests at the original source document level rather than at a summary level of activity (fraud occurs at the source document level, and is concealed at the summary level).

Perform an unannounced cash count, including a review of the check and cash composition. Be observant of all employee activity during the count.

Perform a review of the sequential issue and use of official prenumbered documents and cash register "Z" tapes. Obtain an explanation for missing "Z" tapes.

Perform a review of procedures for all cash register voids, refunds, non-cash credits, cancellations, and adjustments, including proper accountability for these high risk transactions on a management exception list, supervisory approval, and validity of all supporting documents.

Determine whether managers monitor the cash overages and shortages of each cashier. Analyze variances of cash overages or shortages over a selected period of time to identify any adverse trends by any particular cashier or all of the cashiers.

Perform analytical review of revenues for one period to another and inquire about significant fluctuations (either up or down).

Make an inquiry at all banks in the local area for a list of all accounts in the name of the entity (identifies bogus or other off-book checking accounts).

Don't always accept the first plausible explanation given by management for any exceptions noted during substantive testing. Test the explanations provided to verify the accuracy of the information received.

Observe cash receipting operations when visiting decentralized locations. Review the timeliness of deposits from decentralized locations to the central treasurer function. Also review the appropriateness of the cash transmittal system used.

Compare the amount of cash receipts shown at the central treasurer function with the amount of cash receipts recorded at the decentralized receipting locations for the same transaction.

Analyze bank deposits for presence of (1) personal checks from cashiers and other fund custodians (the employee may be "borrowing "money from the entity) and (2) unrecorded revenue checks which were not receipted by cashiers (detects a check for cash substitution scheme).

The position and background of fraud perpetrators are unpredictable and change over time. Their actions also change when revisions are made to the internal control structure. Everyone within the organization has the opportunity to do something irregular.

Most fraud perpetrators use common and simple methods. Be aware of the most obvious fraud indicators. Engage the mind and use your experience. Common sense is your most valuable resource.

Look for a straight line from source to approval to payment when reviewing the processing of documents which serve the same purpose as blank checks (petty cash

documents, travel vouchers, and time cards). All fraud (falsification, alteration, change) occurs after approval when the documents are returned to the source before being processed for payment.

At the heart of every fraud is a missing or fraudulent (falsified or altered) document. Accept original source documents only.

All types of checking accounts, particularly those imprest funds which are routinely reimbursed, are high risk. Be alert for false or altered documents. Fraudulent deposits (laundering of unrecorded revenue transactions) and fraudulent disbursements (issuance of a check to "cash", themselves, a bank, or a fictitious vendor) are the major concern, not the authorized imprest fund level itself.

Computer frauds are no different than manual frauds. All are perpetrated basically the same way.

Comparison of check/warrant payee and amount to the check/warrant register and a review of the actual endorsements are essential steps for the detection of fraudulent or manipulated transactions.

Risk Alerts

RISK ALERT - COUNTY AUDITOR'S OFFICE

After meeting with the Department of Licensing (DOL), an August 25, 1995, letter was sent by DOL to all County Auditor's Offices clarifying procedures for cash handling in the automobile licensing section. Two methods are used: (1) Operator (one person, one change fund, one cash drawer); and, (2) Workstation (cash drawer is shared by multiple cashiers).

> There are good internal controls over cash when the Operator method is used. The bad news is that only a few County Auditor's Offices use this method.
>
> There are poor internal controls over cash when the Workstation method is used. Even considering the automobile licensing section's operator password system, there is no fixed responsibility for funds (and losses, if any) when multiple cashiers use the same change fund and cash drawer. The bad news is that most County Auditors's Officers use this method.

When the Workstation method is used, individual cashiers must have their own separate cash drawer. However, this does not appear to be happening, even after the issuance of DOL's recent letter. Therefore, cash handling procedures should be reviews in the County Auditor's Office during County Audits. In fact, this is a good practice on all audits. The following example is an excellent statement of the effect of this poor internal control procedure.

One County Treasurer trusted his employees and allowed multiple cashiers to use a single cash drawer. Even when we advised him to change procedures, nothing was done. That County Treasurer recently incurred a $1,000 loss of funds, and was not able to fix responsibility for the loss. The interesting thing is that the internal control was changed immediately after the loss. Somehow, the importance of the internal control was now realized. Wouldn't it have been better if we could get the internal control procedures changed before the loss occurred? Think about it (on all audits), because this County Treasurer is not alone.

RISK ALERT - UTILITY CASH RECEIPTING OPERATIONS

Team Yakima Question:

Part of a theft at City of Wapato was through the water and sewer utilities. Cities usually use the stub off the billing as a receipt and they stamp the other copy as paid for the public. The theft could not be isolated to an individual since the cash drawers reconciled and the theft was perpetrated by removing the same amount of stubs as the money they removed. Even though the cash drawers are locked and only one person has access, we cannot assign responsibility since we cannot prove which drawer the theft was out of or who received the stolen money.

Since this affects all cities, should we be recommending that all cities use prenumbered official receipts instead of stubs to isolate the cashier receipting the money and the date of the theft? Or, do you have a better solution? Currently, the only way to know a theft has happened is at month-end when a person complains that they paid their bill last month.

Fraud Specialist Answer:

Before I begin my answer to this important question, let me address an issue which is included within this question. Fixing responsibility for funds is a management responsibility, not an audit responsibility. Therefore, always say (and write) "management could not determine", not "we could not determine" something. That places the responsibility for the internal control structure right where it belongs.

Now for a rather lengthy answer to your question. First of all, the basic system of utility stubs equals the amount of cash received just isn't sufficient to adequately monitor the utility cash receipting function. So, what can we do about it? If we recommend that prenumbered official receipts be issued in a manual cash receipting system, or that transactions be recorded on a cash register of some type (computer or stand alone system), this is a duplication of effort which will be resisted, perhaps vigorously by management, and rightfully so. It's overkill with little or no return. Even if we make this recommendation, it will not be implemented by managers due to the cost involved as well as the lack of perception of a need for this action. By the way, using a cash register is no guarantee that all transactions will be recorded either, because a dishonest cashier will not record the transactions they choose to manipulate. They just don't play by the rules.

We must encourage entities to limit their exposure to this risk. However, cost is a factor in determining what internal controls management will decide to implement. I believe that the cost of using prenumbered official receipts will preclude any action by management. So, if we don't recommend the use of prenumbered official receipts as indicated above, what do we suggest? Here are some things that can be done under the existing system for utility accounts receivable and cash receipting systems.

(1) The "paid" stamp used by cashiers should indicate the date and cashier station (i.e.; cashier "A", "B", etc., not the cashier's name). The station identification should be linked to and identify the cashier, however. These stamps should be controlled, protected, and assigned to

cashiers in the same manner as change funds. Every cashier should have one, including relief cashiers. They should be stored in a safe/vault with the change fund for safeguarding when not in use.

(2) Cashiers should annotate the mode of payment (i.e.; by check or cash) on the retained stub to reconcile cash receipt composition at the end of day/shift. This too is no guarantee that all transactions will be correctly recorded because a dishonest cashier will falsify this information to conceal a check for cash substitution scheme. Thus, mode of payment should be periodically monitored by management for cashier compliance with this procedure by reviewing the actual checks from the cashiers prior to making the deposit. And, cash receipts should be reconciled by management by mode of payment and cashier at the end of day/shift.

(3) The entity should ensure that accountability for funds is fixed to a specific cashier. Cash register passwords may be used for this purpose. But, the entity must also maintain the concept of "one cashier-one change fund-one cash drawer". More than one cashier should not operate from a single cash/till drawer or commingle funds. This condition always results in "no fixed responsibility" when, not if, a loss occurs. When this happens, all of the cashier's reputations/careers have been compromised and have been perhaps irreparably damaged. Managers should never let this event occur in their operations.

(4) Customer feedback serves as the major line of defense against fraud by cashiers. This feedback should never come directly to cashiers (who always fix the problem), but rather should go to a customer service representative/section or other independent party for review and analysis. In addition, these employees must be properly trained to recognize the attributes of fraud. If a customer presents documents to prove that their account was paid even though the accounting system does not reflect this condition, the account should be adjusted (credited) to reflect this payment. However, the entity should not simply "write-off" the fraud. Correct follow-up research, using the documents provided by the customer, should be performed in an attempt to adequately resolve this condition which is either: (a) a collect the money and steal it scheme (the most common fraud in the world); or, (b) a lapping scheme (where the cashier has made a fatal mistake).

a. To resolve a collect the money and steal it scheme, the entity may have to covertly install video cameras to tape/monitor the cashiering function to identify the cashier responsible for this irregular activity.

b. To resolve a lapping scheme, the entity should perform a "slow-pay" test. Customer's accounts which were credited with payments late in the cycle should be selected for review and confirmation with the taxpayer/customer, asking them for verification of the date and mode of their payment. This test will identify customers who paid early in the cycle, but whose accounts were credited late in the cycle (i.e.; a lapping scheme). Accounting records for any questionable day should be thoroughly reviewed for check and cash composition and for any other unusual attribute observed in this step. Exact steps to take will, of course, always be different and be dictated by what is found in this review.

c. Regardless of the circumstances cited in the examples above, the entity should also compare the composition of the bank deposit (from a bank-validated deposit slip showing

composition) with the composition of their cash receipt records to identify a check for cash substitution scheme. They may have to obtain a copy of the deposit slip from the bank's microfilm records to do this. In addition, this step should be routinely performed on a periodic basis to monitor the cash receipting function.

(5) To improve the likelihood of receiving customer feedback when problems do occur, the entity should ensure that the date of customer payment is automatically printed on the billing stub document. Some stubs just reflect the words "payment" and the amount, which is inadequate for this purpose. When the date of customer payment is shown on the billing document, alert customers will possibly notice the lapping scheme attribute when they paid early in the cycle but their accounts were credited late in the cycle.

(6) A segregation of duties problem exists if cashiers have the ability to post customer accounts receivable accounts "paid". This gives the cashier the opportunity to collect the money and steal it, as well as to process a fictitious payment into the system. When this occurs, total credits to customer's accounts will not equal total bank deposits over a period of time. Therefore, we must test for this condition during our audits. Refer to the Accounts Receivable Section in the Fraud Detection and Development Manual (pages 2-17 and 2-18) for the six critical steps that Assistant State Auditors should perform during routine audits of all types of accounts receivable systems.

Is accounts receivable a high risk function? You bet it is. Therefore, you should have accounts receivable systems appropriately prioritized in your audit plans for coverage during every audit cycle.

Why are these internal control procedures important and necessary? The answer to that question is "because accounts receivable systems, such as the utility system used in this example, are where most unidentified/unknown frauds exist today". Under today's method of operation, these frauds will continue to exist unless cashiers get caught by making a fatal mistake. To my knowledge, the "slow-pay" test is the only line of defense against the types of fraudulent schemes described above, particularly a lapping scheme involving accounts where customers pay in cash (currency).

This was a great question by Team Yakima and audit manager Dave Andrews. So, thanks. I love that questioning attitude by auditors. It's a mind-expanding exercise that is healthy for proper professional growth and development. Improved entity internal control procedures will also result from this exchange because I know you're going to share this information with your auditees when you perform future audits.

Are there any other fraud questions out there? If so, send them to me by E-mail. I promise to get you a prompt response via a future Monday Morning Briefing article.

RISK ALERT - SEGREGATION OF DUTIES

The number one internal control weakness cited in all fraud reports is an inadequate segregation of duties. This applies to all activities and functions within all state agencies and local governments.

The root cause of all fraud is an employee's need for money as a result of some financial crisis in their life. These financial pressures can develop anywhere along the income scale --top, bottom, and anywhere in the middle. We can understand why a financially strapped clerk employed in a receipting or disbursing function may have this problem because we see these conditions in a number of fraud cases every year. But this very same problem also occurs at the chief financial officer or executive director levels. No one is exempt. Anyone can create a lifestyle above their income level, regardless of the amount. This ultimately leads to financial ruin.

Employees satisfy this need for money by stealing from their employer. They simply bring this need to work and remedy their problem by embezzling funds from the government. They may choose a wide variety of methods to accomplish this task; but, it's always an inadequate segregation of duties which allows the fraud to be perpetrated, as well as to be concealed over a long period of time.

In addition, we often see greed set in after the scheme has become firmly entrenched in daily operations. Fraud is also addictive, just like drugs and alcohol. Thus, these individuals cannot and will not stop for any reason.

The root cause of fraud inside the organization is an inappropriate segregation of duties for a key employee in either the receipting or disbursing functions. Since this one internal control is at the heart of every fraud which exists today, you must manage or audit with the full knowledge that identifying this menace must be one of your primary missions or objectives in life. Your study of the entity's internal control structure is a good place to start on this mission.

This internal control weakness is present in far too many locations, but is not always dealt with correctly by managers or auditors. You must ask the correct questions about the duties and responsibilities of key employees to find out exactly what they do on the job. The key questions are: "What do these employees: do, sign, approve, certify, authorize, supervise, review, reconcile, etc." These key terms should quickly give you enough information to determine when an employee has too many or overlapping responsibilities which create a segregation of duties problem.

Trusted employees simply ignore or compromise internal controls to perpetrate their crime. When it's not possible to segregate duties between two or more employees, management officials must establish a monitoring program for this key employee which effectively accomplishes a segregation of duties without hiring another individual to perform this task.

> For cash receipting functions, someone independent of the function should periodically review the check and cash composition of daily bank deposit to a bank validated deposit slip which lists the check and cash composition of the actual deposit.

> For cash disbursement functions, someone independent of the custodian of bank accounts or the general disbursement system should perform (preferably) or otherwise correctly review the monthly bank reconciliation.

The purpose of this monitoring process is to determine if the internal control structure operates as designed, and when, not if, public funds have been misappropriated. This critically important step serves as both a detection mechanism for management and a deterrent mechanism against unauthorized or irregular activity by employees.

Lack of monitoring (i.e.; review and oversight activities) of key employees by management officials is one of the biggest problems which exists in the state of Washington today. Therefore, this issue must be appropriately dealt with by both managers and auditors.

Think about this alarming fact as you go about your daily management or audit duties.

> Every fraud case that is currently in existence, and that will be detected and reported in the coming year, is going on right now because of an inadequate segregation of duties somewhere within the entity.

Is it happening to you where you work or audit?

RISK ALERT - CHECK FOR CASH SUBSTITUTION SCHEME

The number one cash receipts fraud after accountability records have been established (i.e.; manual cash receipt forms have been issued or cash register recordings have been made) is a check for cash substitution scheme. How big of an impact does this type of fraud make? For the 9-year period (1987-1995), check for cash substitution fraud accounted for 9% of our total cases and 24% of our dollar losses. Thus, this is an important type of fraud for everyone to understand.

In this scheme, checks from unrecorded (i.e.; no receipt written by the cashier) cash receipt transactions are substituted for cash from recorded cash receipt transactions. When this occurs, the check and cash composition of the bank deposit will not match the composition of the mode of payment information listed in the cash receipting system. Thus, recording mode of payment (i.e.; payment by either check or cash) on cash receipt forms and in cash register systems is essential for this test to be properly accomplished. This test can be performed without the mode of payment information being present; however, it's a costly process.

Cashiers always find a way to mark the manipulated customer's account "paid" in some way to eliminate customer feedback, one of the most common ways these frauds are actually detected by management officials. If they don't, they get caught real fast.

Auditor's must verify total accountable cash receipts by mode of payment to a bank validated deposit slip which lists the check and cash composition of the actual deposit. If the entity does not already do so, they should prepare bank deposit slips in duplicate for the bank to validate. This is both cheap and easy to do (i.e.; very little cost to implement this control procedure).

If duplicate bank deposit slips are not available, auditor's cannot complete the review of the cash receipting function until they have obtained a copy of the actual bank deposit slip from the bank's microfilm records. This step is costly. But, it's absolutely essential because the actual bank deposit slip and the subsequent detail of checks and cash included in the deposit always proves the case when fraud exists.

But, this step is also essential because of the variety of ways that employees perpetrate this fraud. Employees have perpetrated this fraud as cashiers at decentralized cash receipting locations, as couriers transporting funds from the decentralized location to the central treasurer function, as cashiers at the central treasurer function, and as couriers transporting funds from the central treasurer function to the bank.

So, take it from one who has seen enough of these frauds to know better, verifying total accountable cash receipts to a bank deposit slip which shows only the total amount of funds deposited (i.e.; no composition) just isn't good enough anymore because it simply misses the fraud.

Employees almost always substitute checks for cash on a one-to-one relationship (i.e.; a $50 unrecorded check is usually substituted for $50 in cash). This makes it easy for them to operate this scheme. But, we have had one case where the individual substituted checks for an amount

of cash which was approximately 50% less, with a receipt being issued for the difference. Taxpayers checks paying full-year property taxes at the beginning of the year were used in this scheme. Since only first-half property taxes were due when these payments were received, the County Treasurer issued a receipt for the first-half property taxes amount, deposited the check for the full-year payment, and took the difference in cash (i.e.; the amount of the second-half property taxes). These funds were borrowed for about six months and repaid by the County Treasurer when the second-half property tax payment was due (i.e.; borrowing).

A new development has arisen in this scheme from a number of fraud cases during the past several years. When individuals process large checks in a check for cash substitution scheme, there often isn't enough cash on-hand in a single deposit to manipulate the transaction on a one-for-one relationship as described above. However, this does not deter the perpetrator. When these large checks are substituted, cash and other smaller checks which have been properly receipted are removed from the deposit. These smaller checks are then substituted for cash on subsequent business days when there is a sufficient amount of funds available for this purpose. This turns into a nightmare and makes a very complicated case.

A common and related problem encountered is that "Rediform" cash receipting forms are often used rather than official prenumbered cash receipt forms with the entity's name printed on the document. Auditor's should identify and eliminate the use of "Rediform" cash receipting forms in all state agencies and local governments, because their use allows employees to steal money. Books of these cash receipt forms can be obtained by anyone at a wide variety of retail office supply stores. They are then used against the entity (i.e.; one book for the employee for cash transactions, and one book for the entity for check transactions) when frauds are perpetrated.

Unannounced (surprise) cash counts by entity managers and auditors are essential to detect a check for cash substitution scheme in progress. This step is important because it's the one and only opportunity for anyone to determine exactly what the employees are actually doing during normal business operations. Variances between what employees actually do and what they should be doing, according to the entity's authorized policies and procedures, should be noted for further review and analysis during the audit.

During the unannounced cash count, auditors should not only verify the composition of cash receipts and bank deposits, but also review the sequential use of prenumbered documents and cash register "Z" tapes. Methods used to record and authorize other high risk transaction types such as voids, paid-outs, refunds, non-cash credits (primarily in court systems), and cancellations and adjustments (primarily in accounts receivable systems) should also be reviewed.

Now that you have included this information in your auditor's tool box, you'll be prepared to de an even better job of deterring and detecting check for cash substitution fraud schemes. If you do your audit work correctly as described above, you'll find these frauds automatically. So, good hunting!

RISK ALERT - CHECKING ACCOUNTS

The number one cash disbursement fraud involves an individual who writes checks or warrants to: (1) "cash"; (2) themselves; (3) a bank (i.e.; to purchase a cashiers check or money order); or, (4) to a fictitious vendor. The ultimate objective of all such schemes is to first get the check or warrant, and then cash it to use the money for personal purposes. Employees will steal checks from both revenue and disbursement systems.

a. The first three above conditions usually occur in checking accounts of all types (i.e.; depository, trust, advance travel, purchasing, petty cash, etc.). For checking accounts, the authorized imprest fund level is not always the major concern. Rather, it's the level of activity for fraudulent deposits and fraudulent disbursements within the account that is the "red flag" which sounds the alarm.

These checking accounts are high risk because they are so vulnerable to manipulation by employees who launder both revenue and expenditure transactions through them. All of the following methods have been used in fraud cases:

(1) Establish a "bogus" bank account in the name of the entity, deposit the checks, and issue checks to "cash" or to themselves.

(2) Use a bank account with a name similar to the name of the entity, deposit the checks, and issue checks to "cash" or to themselves.

(3) Deposit checks into an imprest or trust fund and issue checks to "cash" or to themselves.

(4) Deposit checks into a personal bank or credit union account.

(5) Make a "cash back" withdrawal from a bank deposit for any type of bank account.

(6) Cash the checks at a bank or vendor.

(7) Use a check for cash substitution scheme in the entity's normal bank deposit.

(8) Alter the amount of checks (increased) and remove an equivalent amount of cash from the till drawer (and deposit).

For most types of checking accounts, there is no authorization and approval process. The custodian simply signs the checks. Even when there is a dual signature process, it's easily compromised. Either checks are pre-signed by one individual, or one person signs the checks and has access to the facsimile signature plate of the other individual. If not, all fraud occurs after approval through alteration and falsification of the checks after signature.

b. The final condition above (i.e.; writes checks or warrants to a fictitious vendor) usually occurs in the warrant disbursement system and is very difficult to identify; but, it can be done. Knowledge of the entity is your best defense. The critical element in fraud cases involving disbursement schemes involves an employee who has both input and output capabilities (i.e.; the ability to prepare fraudulent input document, and then obtain the resulting warrant). This condition exists in all disbursement fraud cases and is "the kiss of death". Thus, anyone with input and output authority has a segregation of duties problem that must be dealt with promptly. This can occur in both the accounts payable function and the payroll function where often only one individual does everything. Duties of these individuals can easily be revised. The accounts payable clerk should get the output from payroll, while the payroll clerk should get the output from accounts payable. This easily solves the segregation of duties problem with no added expense. But the fraud can still be perpetrated by having the warrants mailed to the perpetrator, perhaps through a false vendor using a post office box mailing address.

For both scenarios listed above, someone independent of the custodian of bank accounts or general warrant disbursement system must perform or review the monthly bank reconciliation. This is the critical control which must be relied upon to detect these frauds. These individuals must also be properly trained and know how to detect irregularities. Comparison of check or warrant payees and amounts to the check or warrant register, and review of the check or warrant endorsement are essential. These steps will detect almost all disbursement frauds in either the private or public sectors.

The major attribute of all cash disbursement fraud is "too high" or "too much". Recorded expenditures are up when fraud is present. The accounting transaction for fraud is to debit expense (or assets) and credit cash. Fraud processed through asset accounts is dumb because the perpetrator must deal with the 'shortage" from year to year. Most fraud is processed through expense accounts because irregularities disappear at year-end. Fraudulent disbursements are buried in accounts with a high volume of activity or with a high dollar amount to conceal them from discovery. A comparative analysis of disbursements is usually the first "red flag" noted. Other steps include balancing check or warrant registers, reviewing check or warrant voiding procedures, and reviewing storage and issue controls for these negotiable instruments.

RISK ALERT - COLLECT THE MONEY AND STEAL IT

The number one cash receipt fraud before accountability records are established is for cashiers to collect the money and steal it. No accountability records are created (i.e.; manual cash receipt forms or cash register recordings) when customers pay cashiers for some type of user fee. These frauds can occur at all activities and functions within all state agencies and local governments. They usually occur at decentralized cash receipting locations where cashiers often work alone.

Missing revenue streams is a common element in these frauds. All, or practically all, of the revenue from a particular source is stolen. Cash is simply taken. Checks are laundered in a variety of ways to negotiate them to get the money for personal use. You must ensure that all sources of revenue are included in the annual budget. But, establishing control over checks which arrive through the mail, the highest risk transaction which exists anywhere in the private and public sectors, is also essential. You must identify and eliminate all off-line accounts receivable systems, because the outstanding balances, when collected, represent "free" money. No one will know if payments on these account balances are missing, and no one trusts the accuracy of these recorded accounts receivable balances either. Thus, fraud is easily concealed in these accounting records and systems. Therefore, two individuals should open the mail, make a log or record of the transactions, turn these checks over to the cashier function, and then reconcile the log to daily cash receipts and the bank deposit to ensure that all transactions have been properly accounted for and controlled.

The major attribute for all cash receipt frauds is "not enough" or "too little". Recorded revenue is down when fraud is up. A comparative analysis of revenue is usually the first "red flag" noted. But, while analytical review procedures will detect a drop in reported revenue, this step will not necessarily detect the absence of revenue from a particular source or the theft of a constant amount or percentage of these revenues.

Identify any alternative records which establish a reasonable amount for the revenue source. Observe cashiers during normal business operating hours. If possible, this should be done without their knowledge. Use of controlled batches of transactions and documents is an effective step to use when warranted by the circumstances. If all else fails, make arrangements with a law enforcement agency to video-tape cashier operations to determine the cause for variances noted. These agencies often use marked money during investigations.

When a key internal control is not used by the entity, you mush now ask yourself: "What is the compensating control that is used by the entity that takes care of this issue?" This is the most troublesome area we're experiencing statewide, because entity's are having trouble actually determining what they should do. And, the remedy for the compensating control can vary. It can be anything from the point of the original internal control procedures (that isn't done) all the way to the end of the accounts receivable system in the area of delinquent balances (far, far away). So, what works for one entity may not work for another. Actual practice will dictate what is eventually done about this internal control procedure.

Take SAO as an example. We bill our audit services to the entities from the Fiscal Office each month (accounts receivable system). The mail containing the payments arrives at the Legislative

Building. The envelopes are opened and then tossed into a box for the Fiscal Office. Later in the day, they are sent through campus mail to the GA Building. No log or record of these checks is ever made. We don't do this control either. So, where is the compensating control? It's in the accounts receivable system (customer feedback). If someone were to take one or more of those checks, we would send out a dunn letter asking for payment of a delinquent billing. The entity would tell us they aid their bill. We could obtain a coy of the redeemed check from the entity's bank. That document would tell us what happened to the check, as well as establish the trail to the party responsible for this action. Can you stop it from happening? No. But, you can catch it promptly when, and if, it does occur. That's as good as it gets. Do we need to apply any further internal controls over this area? Probably not. If we did, it just wouldn't be cost effective. And, this is the major resistance issue that you will get from entity management about this internal control issue. So, just be prepared with a cost effective answer/remedy as the compensating internal control which should be implemented when checks are not properly logged in the mail room. The bottom line in this example for SAO, and for any entity for that matter, would lie in the resolution process for delinquent accounts receivable accounts because any irregular activity might be concealed in this area. We would have to look very carefully at the write-off of account balances and any unsupported adjustments to accounts. Management officials in any entity would have to do the very same thing. We should then review their work to determine if it is sufficient for audit purposes.

RISK ALERT -- SPECIAL FUNDS

There are at least two special fund operations in state and local government. They are:

(1) Confidential Funds. These funds are in the custody of law enforcement agencies, and are used primarily to conduct undercover drug investigations. The fund we normally encounter in local government is located in the County Sheriff's Office and the City Police Department. Access to these confidential funds is restricted within these law enforcement agencies because of the sensitive nature of the transactions. Therefore, they appreciate the fact that we similarly restrict access to these funds by auditors from our office.

While we have been auditing these funds routinely during county and city audits, funds in the hands of Joint Task Forces may have been overlooked. The largest participating member of the task force is usually designated the host government which controls any funds they administer. So, be sure to include the operation of Joint Task Forces in the audit plan for these governments.

(2) Antiprofiteering Funds. These funds are in the custody of county prosecuting attorney's offices, and are used primarily to conduct undercover antiprofiteering investigations. These are also referred to as racketeer influenced corrupt organization (RICO) investigations. Since these funds have only existed for the past several years, our risk is that it might be omitted from the county audit plan. Contact your county prosecuting attorney to determine whether such a fund exists.

Funds for future operations of these undercover operations come from court assessments made against convicted criminals in drug and profiteering cases. The original source document for these transactions is the assessment listed in the restitution order for each case. The courts maintain accounts receivable records on these assessments until the debt is collected. The funds are then transmitted to the law enforcement agency or prosecuting attorney's office.

These special funds must be authorized imprest funds of state and local government, and must be accounted for in a Special Revenue Fund. Once properly authorized, the funds may be kept in checking accounts, cash funds, or a combination of both. These special funds are automatically high risk funds.

Revenue. Funds from the court must be routed through the treasurer's office for accounting purposes. The most common weakness noted in the past has been that the courts have sent this revenue directly to the law enforcement agency or to the prosecuting attorney's office. Success comes only from a coordinated effort by the court, law enforcement agency or prosecuting attorney's office, and treasurer's office. You may have to be the catalyst for this action to occur.

Disbursements. Expenditures from these funds may not have any supporting documents other than the case file entries maintained by the individual handling the case. Therefore,

it's essential that we verify the authenticity of these transactions by reviewing actual case file information during audits.

Guidance for the operation of these funds is as follows:

Imprest funds: Budgeting, Accounting, and Reporting (BARS) Manual, Volume I, Part 3, Chapter 3, Page 23.

Confidential funds: BARS Manual, Volume I, Part 3, Chapter 12, Pages 15-16.

Antiprofiteering funds: Revised Code of Washington 9A.82.110. This statute mentions a county antiprofiteering revolving fund; however, it does not provide any guidance for operating the fund. Since this fund must operate exactly like a confidential fund, the guidance in BARS Manual, Volume I, Part 3, Chapter 12, Pages 15-16 applies.

RISK ALERT -- PROPERTY AND EVIDENCE ROOMS

There are a number of property and evidence room operations in state and local government.

(1) Law Enforcement Agencies. We routinely audit property rooms in the County Sheriff's Office and the City Police Department where property seized in criminal cases is held as evidence until trial. This property includes currency, drugs, weapons, and other miscellaneous assets. All such property must be inventoried at the time of seizure and secured in property rooms. Access to these assets must be limited, safe and vault combinations must be safeguarded and routinely changed, inventory records must be maintained for accountability purposes, and disposition records must be retained on file for audit. Certificates of destruction for these assets must be signed and witnessed by two people.

Over the years, we have had a number of fraud cases involving losses of currency from law enforcement agency property rooms. Some cases had fixed responsibility for the loss amount, and others did not. We must evaluate whether management can fix responsibility for the assets under their control to a specific individual at all times. This may be a challenge when a number of people have access to the storage location.

(2) Other Functions. A number of other functions have similar responsibilities for controlling seized property and evidence. The rules listed above for the control of assets in law enforcement agency property rooms also apply to these functions.

Joint Task Force. The largest participating member of a Joint Task Force is usually designated the host government and controls any property seized.

Prosecuting Attorney. Property is seized by the County Prosecuting Attorney in antiprofiteering cases.

Courts. We routinely audit the financial activities of all types of courts, but may be overlooking the security of, and accountability for, assets retained as evidence in court proceedings. Custody of assets may be transferred from law enforcement agencies to the court.

A recent report about problems in a court vault included the following: the property room was in disarray, drug containers were open, and weapons were not tagged. There was another case where a janitor gained access to a court vault and sampled currency and drugs held in evidence. The janitor found the vault combination written down in the office. The court was not aware of this loss until the janitor shared this information with a law enforcement agency during a confession for another crime.

Coroner. Property of deceased individuals is often seized by the Coroner. Claimed property is returned to heirs. Unclaimed assets are transferred to the County Treasurer.

Treasurer or Other Trustee. Unclaimed property from a variety of sources must be safeguarded by, and disposed of, by the Treasurer. Depending upon the type of property, other trustee organizations may be involved. These include at least the State Treasurer and the Department of Revenue. Some funds are transferred to the permanent common school funds of the state and the state general fund for the public safety and education account. The Department of Natural Resources may also lease and sub-lease or rent property escheated to the state of Washington.

There are a number of references for the operation of property and evidence rooms. Some key terms to research in the index to the Revised Code of Washington (RCW) include: foreclosures, forfeitures, escheats, search and seizure, and surplus property. Some citations include: RCW 9A.83.030, Chapter 10.105 RCW, Chapter 11.08 RCW, RCW 11.76.220, Chapter 36.24 RCW, RCW 43.10.270, Chapter 46.12 RCW, RCW 48.31.155, and RCW 69.50.505.

RISK ALERT -- GHOST EMPLOYEES

I recently received an inquiry about ghost employee testing from Team Yakima. The recent Fraud/High Risk QCR identified this as one of the areas within the payroll function which was getting little or no attention during audits (specifically the fraud/high risk bucket). Key questions and responses follow.

Should ghost employee testing be performed on all audits? The timing and frequency of specific audit tests is always a team decision. There are plenty of payroll tests that can be accomplished on any audit. While everything does not need to be performed during each audit, key tests can be cycled over a period of time to ensure that adequate coverage is given to the payroll function.

Should ghost employee testing be performed in certain entities and not others? This fraud could occur anywhere and at any time, even if the entity has a good segregation of duties in the payroll function and payroll warrants are properly approved prior to issuance. The type and size of the entity makes no difference. Therefore, this is a good test to perform at any entity. The case below is a good reason why.

In the cases we know about, the ghost employees were actually hired by entity managers. Therefore, all employees had an official file in the personnel department. As a result, a test to determine if all employees on the payroll also have a personnel file will not necessarily detect a ghost employee. In these cases, the only problem was that the employees never came to work. But, the supervisor who hired these individuals signed their time cards and approved them for payment. The supervisor then picked-up the payroll warrants from the payroll function, distributed them to the individuals, and then split the proceeds from this illegal activity with them. When this event occurs, the payroll warrants are often endorsed by both parties. Where pick-up and hand delivery of payroll warrants is a standard payroll practice, this condition is a higher risk than if the warrants are actually mailed to the employees or sent to their banks via electronics fund transfers. But, fraud can occur in any of these situations.

How do we detect a scheme similar to the above case scenario? The ghost employee test is designed for this purpose. The test can be performed more than one way.

(1) Conducting a ghost employee test of all entity employees is one way. This test can be easily performed in small entities. In fact, we often do this during these audits but fail to document the work in our workpapers. Thus, we don't always take credit for everything we know about the entity. But, this test may be time consuming in larger entities. For example, a new examiner with limited audit experience conducted this test at a county. It took 8 hours. The primary problem experienced was trying to identify employees in certain functions, such as those employees on the "grave yard" shift at the jail and certain work crews in the Public Works Department.

(2) Conducting a ghost employee test of all employees in a particular department or function or activity is another way. This work can be easily accomplished while the examiner is on-site performing other departmental tests.

How is the ghost employee test conducted? There are two ways to perform this test.

(1) Conduct a payroll payout. All payroll warrants (or electronic fund transfer documents) are obtained by the examiner and distributed to the employees. I never recommend this approach because it can easily cause an unnecessary employee morale problem. The resulting complaints are never worth it.

(2) Use a payroll list. Obtain a list of all payroll warrants for a specific pay period. Visit the departments to conduct the test. Observe employee work stations or ask an employee who does not perform payroll duties (i.e.; does not process time sheets or leave slips) to review the payroll list and confirm that all employees actually work in the department.

What category of employees are the highest risk? Probably at least the following:

(1) Part-time employees. These individuals are employed throughout the year in a variety of departments. But, they may be concentrated in the parks and recreation department during Summer months. Thus, you might test these employees during this period of time.

(2) Employees who terminate employment with the entity. This could also involve employees in retirement systems. In these cases, no one notifies the entity when the individual dies. Or, after receiving the notification of death, an employee does not process it and merely changes the individual's mailing address to one that they control, usually a post office box. Thus, payments continue. The primary test to perform is to determine if there are any payments recorded in the system after the termination or death date.

The reason these two categories are the highest risk is that entity procedures for terminations may not be very effective. Since these individuals already have been hired and have a personnel file, a department supervisor only needs to submit a time sheet for the individual (falsification of a public record) in order to obtain the funds from this scheme. Hopefully, ex-employees will complain about any pay irregularities when they receive their annual W-2. But, this may not actually occur unless the individual maintains accurate pay records of their own. Since this isn't always the case, a small overpayment amount may not be noticed at all.

What are some other attributes that could be related to ghost employees? Some additional "red flags" are as follows:

(1) Management officials or internal auditors do not periodically perform a ghost employee test.

(2) Total payroll expenses exceed the amount of payroll reported on W-2/W-3 forms filed with the Internal Revenue Service.

(3) The quarterly Form 971 filed with the IRS indicates routine refunds (i.e.; over-deposits) to the entity.

(4) Time sheets or other time records are not signed by the employee.
(5) Payroll warrants are issued to individuals for large or even dollar amounts.

(6) Payroll warrants are endorsed by more than one person.

(7) Management does not verify that mid-month payroll draws are deducted from end-of-month payroll. This primarily applies to small entities.

(8) Excluding overtime, total payroll for key employees exceeds the authorized level.

(9) Retirement warrants returned as undeliverable by the post office are held in the retirement system office and are not dealt with promptly.

(10) Warrants for retirement fund withdrawal transactions are returned to the retirement system office for distribution.

(11) An address change in a retirement account is immediately followed by a request for payment.

Since “red flags” vary based upon the circumstances of each case, this isn’t necessarily a universe of attributes. There can always be more. But, this is certainly a sufficient amount of information to assist you in performing the ghost employee test in the payroll function during routine audits. I hope you find this information useful as you conduct future audits. And, good luck!

RISK ALERT -- CHECK/WARRANT ENDORSEMENTS

I recently received an inquiry from Team Tri-Cities about the information shown on the reverse side of canceled checks and warrants (negotiable instruments). The input I received was as follows: "We look at the back of a lot of canceled checks, but mainly for endorsements and deposit information. What do all those other numbers mean? Is it possible that those other numbers could be of audit benefit?" My response follows.

The primary information shown on the reverse side of negotiable instruments includes the following:

(1) Endorsement. Negotiable instrument endorsements by an individual or the entity are the primary data element we review during audits. We normally verify this information for agreement between the endorsement on the reverse side of the negotiable instrument and the name of the payee on the front side of the document as well as the supporting voucher documentation. Watch for alterations of the payee name on the front side of these documents. Some of the most common alterations include typing an individual's name over the top of the entity's name on the payee line, changing the payee name by using "white out", and completing the spelling of a company name, such as IBM or UPS, by changing the payee name to IBMitchell or UPSampson. Using only initials as the payee name on negotiable instruments represents a high risk for all entities because this information is so easily altered. Thus, this procedure should be discouraged. All of the above alterations represent "forgery", a felony in the state of Washington.

(a) If the negotiable instrument is a revenue check included in a bank deposit of the entity we're auditing, there should be a restrictive endorsement on the document indicating the name and account number of the organization. Almost all checks irregularly endorsed by fraud perpetrators violate this principle to complete the fraudulent act. So, make sure the endorsement you're reviewing includes the phrase "For Deposit Only". One such irregular endorsement included the use of a rubber stamp indicating the name and address of the entity (such as would be used to stamp the return address on a mailing envelope).

(b) If the negotiable instrument is a check included in an individual's bank account, there may not be any endorsement on it at all. While a US Treasury check must be signed by the individual, checks made payable to the person who is a signatory on the bank account do not even have to be signed (endorsed) by that individual in order for them to be further accepted and processed by the financial institution (i.e.; bank(s), credit union, etc.). If the individual makes a "cash back" withdrawal of funds from a deposit including negotiable instruments, the personal endorsements shown on these documents should not include the phrase "For Deposit Only".

(c) There may be a second endorsement shown on a negotiable instrument such as "Pay To: (Name and/or Account Number)". These endorsements are automatically high risk because this is a "red flag" indicating a potential fraudulent condition, especially on a negotiable instrument for payroll.

(2) Automated Teller Machine (ATM) Code. There may be an ATM Code shown in the endorsement section of some negotiable instruments. This code is usually printed in big, bold, alpha-numeric print. The ATM Code is used to locate the transaction when microfilm research is performed by the financial institution. This information is primarily used by financial institutions rather than auditors; but, the fact that the document was processed through an ATM may be a significant data element for auditors during a fraud investigation.

(3) Initial Proof Endorsement. The proof endorsement includes the name of the initial financial institution which processed the negotiable instrument and the date the transaction was deposited. This information is usually directly under the individual's or entity's endorsement. This information is recorded by the proof machine at the financial institution and may include the date, the name and address, the phrase "Pay Any Bank", the "American Bank Association (ABA) Number" identifying the financial institution, and the "Spray Number". The proof endorsement is usually printed in purple ink from left to right across the reverse of the negotiable instrument (horizontal) and looks like a rubber stamp; however, the spray number is printed along the side of the proof endorsement from top to bottom of the document (vertical) and looks like a "dot matrix" series of numbers. However, the proof endorsement may also be printed horizontally on the document. The date is shown with either the proof endorsement or the spray number, but not usually in both of these data elements. The spray number is used by financial institutions to locate the transaction when microfilm research is performed, and is not further used by auditors. However, we most often use the date of the deposit element of the proof endorsement to verify the timing of the transaction during fraud investigations. The proof of endorsement (including all of it's components as described above) and the spray number are always paired together and should be treated as one data element on the negotiable instrument.

(4) Subsequent Proof Endorsement. The name of any subsequent financial institution which processed the negotiable instrument will also be shown. This identification information is the same as described above for "initial proof endorsement", and also includes the spray number. Again, the spray number is used by financial institutions to locate the transaction when microfilm research is performed, and is not further used by auditors.

(5) Teller Machine Identification. When a negotiable instrument is acted upon by a financial institution teller, a "line of print" indicating several data elements about the transaction is printed on the document by the teller's machine. This information is very similar to the line of print reflected on the typical bank deposit slip, and may be on either the front or reverse side of the negotiable instrument. When deposits are processed by tellers, they insert the deposit slip into their processing machine. Descriptive information printed on the document includes the bank name, date, time, teller identification number, bank account number, type of transaction described either in words or codes, and the amount of the transaction. You will have to obtain an explanation for any codes used on documents you review because they vary by financial institution. This line of print is also used as a research tool by financial transactions when documents are subsequently questioned. We're all comfortable with this line of print on deposit slips; but, when you see this same line of print on documents, it means the negotiable instrument was cashed or otherwise processed by a teller. Look very carefully for this significant data element on negotiable instruments, because this line of print is usually a "red flag" identifying an irregular transaction.

Well, I believe that just about explains all those numbers shown on the reverse side of negotiable instruments. From time to time you may even find additional data elements printed on these documents. If you have any question about those data elements, you can always obtain an explanation from your financial institution. As explained above, some of these data elements are used for audit purposes, such as the endorsements, date of deposit, financial institution involved, and teller "line of print". However, most of the other data elements shown on negotiable instruments are used only by financial institutions for research purposes.

I hope you find this information informative and useful as you conduct future audits. And, thanks to Team Tri-Cities for sending in this inquiry.

SAMPLE REVERSE OF WARRANT/CHECK (ENDORSEMENT)

Endorsement (Horizontal)

John Doe (Signature)	OR	Pay To The Order Of (Bank Name)
Bank Name -- Account Number		For Deposit Only -- Account Number
For Deposit Only		Name of Entity

OR Pay To (Name), Bank Name, and Account Number (Second Endorsement)

Automated Teller Machine (ATM) Code (Horizontal)

APO 806 COURT

First Bank Proof Endorsement (Initial Transaction Processing) (Horizontal/Vertical)

Bank Identification	Date of Transaction	Spray Number (Vertical)
125102906 (ABA Number)	Dec 20 96	Date Sometimes Shown
Bank Name and Address		46100089 (Dot Matrix Printing)
Date Sometimes Shown		

Subsequent Bank Proof Endorsement (Bank Account Location) (Vertical)

DE '96' 21 (Date)	Spray Number (Vertical)
135000024 (ABA Number)	Date Sometimes Shown
Bank Name and Address	34074967 (Dot Matrix Printing)

Bank Teller Line of Print (Vertical)

9005 0028 12/20/96 14:36 $50.00 CC 0000000001 Bank Name

Description of Typical Data Elements in Line of Print (Vertical)

9005 0028 (Bank Teller Identification)
12/20/96 (Date) 14:36 (Time) $50.00 (Amount)
CC (Cashed) -- CKDEP (Check Deposited) --Transient Check ATM -- Other Codes (Varies)
0000000001 (Transaction Number) Bank Name

RISK ALERT --MONEY LAUNDERING ACTIVITIES

Money laundering is an important area for all auditors to understand because fraud perpetrators steal checks and warrants more frequently these days than they do actual currency. This is often hard for both managers and auditors to understand. Why? Because most of us just don't believe negotiable instruments can be stolen and endorsed. But, that is exactly what is done in order for the perpetrator to receive the proceeds from their illegal act.

The major cause of this alarming trend is opportunity coupled with management's lack of control over negotiable instruments. This is particularly true for checks which arrive through the mail. As you might expect, these checks are the highest risk transactions within the entity. There are two basic approaches to this problem.

(1) Cash Receipts. Controlling all revenue checks, including those which arrive through the mail, is a critical internal control issue. One way to do this is to have two individuals open the mail, make a log or record of the transactions, turn these checks over to the cashiering function, and then reconcile the log to the daily cash receipts and the bank deposit to ensure that all transactions have been properly accounted for and controlled. The first complaint from management officials is that this process is too costly. But, the two individuals that are needed for this process do not have to be employed for the express purpose of performing this task. Since any two people will do, anyone from another function can easily assist in this task on a temporary basis, such as at a specified time each day. If this internal control is not implemented, we must search for an alternative control which now accomplishes this same objective. This is often very hard to do. In an accounts receivable system, this alternative control could be as far away as monitoring non-cash credits, cancellations, adjustments, and other types of account write-offs (i.e.; all negative cash transactions). But, this is far removed from the cash receipting function. So, each case will have to be evaluated on its own merits. An alternative solution to this problem is to use a bank lock box for funds arriving from large and repetitive revenue streams. When this alternative is implemented, entity employees do not perform these cash receipting tasks.

(2) Cash Disbursements. Another solution to this problem is to have someone independent of the custodian of any bank account or general disbursement system perform or review the monthly bank reconciliation. However, this disinterested party must be properly trained and know exactly what to look for (red flags) when they review all canceled/redeemed checks and warrants for irregularities. And, the reconciliation must be accomplished in a timely manner (i.e.; within 30 days from the date the bank statement is received) and with the negotiable instruments present for review and analysis.

Finally, an irregular check or warrant endorsement is at the heart of each fraud. Once you've seen it done, you realize just how easy it is to misappropriate funds by using checks. There are a number of methods used by fraud perpetrators to launder entity revenue and disbursement checks and warrants. All have been detected in fraud schemes in a wide variety of entity types throughout the state.

Perpetrators launder negotiable instruments inside the entity by:

(1) Using a check for cash substitution scheme in the daily bank deposit. Currency is simply stolen. In addition to ordinary theft, lapping schemes are often involved.

(2) Making irregular deposits into and subsequent withdrawals from an authorized bank account with a name similar to the name of the entity, such as an employee fund. The perpetrator deposits negotiable instruments to and from the entity into this bank account and issues checks to themselves to obtain the funds. Banks do not question the payee name listed on these checks when deposits are made because they look and sound like they belong in the account, even though they actually do not.

(3) Making irregular deposits into and subsequent withdrawals from an authorized bank account used within the entity (i.e.; general depository, imprest, trust, etc.). The perpetrator simply issues checks to themselves to obtain the funds or pays their own personal bills from the account. When reimbursements of these funds are involved, the custodian often falsifies the supporting documents for individual transactions as well as the actual reimbursement report. In addition, all checks which have been issued for personal purposes during the reporting period will not be submitted for reimbursement. Thus, the numerical sequence of the checks reimbursed will not be complete.

(4) Making a "cash back" withdrawal from a deposit for any type of bank account at the entity. In these instances, the bank deposit slip with the employee's signature will probably not be on file for your review. A false duplicate bank deposit slip will be retained on file for management and audit review. However, it will not be bank-validated. The perpetrator prepares a deposit for an amount greater than required for the day and withdraws the excess amount to make the "net" deposit equal the amount of recorded accountability for the day. At first glance, everything will appear to be in order. But, obtaining a copy of the actual deposit slip from the bank's microfilm records will detect this fraudulent act.

(5) Altering checks by increasing the amount and removing an equivalent amount of currency from the till drawer and subsequent daily bank deposit. Customer feedback from these alterations usually terminates this scheme promptly.

Perpetrators launder negotiable instruments outside the entity by:

(1) Making deposits into a "bogus" bank account in the name of the entity. This bank account is usually established by falsifying the name of an entity official on the signature card when the account is initially opened, as well as any other supporting document the bank might require, such as an ordinance or resolution authorizing the account. The perpetrator then deposits negotiable instruments to and from the entity into this account and issues checks to themselves to obtain the funds.
(2) Making deposits into their own personal bank or credit union account. The perpetrator then uses these funds for personal purposes such as to pay bills, etc.

(3) Cashing the checks at a financial institution or business/vendor. These actions are possible simply because the individual is well known to the employees of these organizations. They do this as a convenience to the individual, and do not actually realize that they are assisting the perpetrator when funds are misappropriated from the entity (unwitting co-conspirator).

So, a word to the wise should be sufficient. Don't be complacent about check processing within the entities you audit. A recent case study involving an accounts receivable fraud (lapping scheme) in a water district clearly emphasizes this fact. After I counted the cash at the entity (i.e.; the petty cash and change funds), the accounting clerk informed me that I was finished and that she needed to get back to work. What was her job? Processing both cash and check payments into the accounting system (i.e.; posting the accounts "paid") and making the daily bank deposit, an obvious segregation of duties problem. When you encounter this condition, you must determine what the effect of this internal control might be. This will often require some extraordinary audit testing on your part.

The accounting clerk expected me to leave her work area and proceed with other tasks on the audit. However, it was immediately and painfully obvious that there were plenty of cash receipts in the clerk's work area, mostly in the form of checks, which had not yet been processed. They also needed to be immediately accounted for and controlled. After counting these funds, posting the accounts "paid", preparing the accounting reports, and making the bank deposit, I discovered that the accounting clerk had over $50,000 in uncontrolled cash receipts in her work area on that day. The operative word here is "uncontrolled", because this is another major internal control weakness which allowed the largest lapping scheme in this state's history to occur and not be detected by management in a timely manner. The case isn't over yet; so, all the information isn't available right now. But, it will be provided to you in subsequent accounts receivable training. This fraud was detected by Team King County while performing cash receipts testing during a regular audit. So, congratulations to the audit staff for this fine discovery!

I hope you find this information to be informative and useful as you conduct future audits.

RISK ALERT -- UTILITY ACCOUNTS RECEIVABLE

Another Utility Accounts Receivable Fraud Detected.

A small city recently detected a water utility fraud case (Eden utility accounts receivable system environment). The city determined that currency from four delayed deposits was missing, confronted the utility clerk about the shortages, and obtained a confession. Our audit determined the utility clerk used two methods in this scheme.

(1) **Utility customer accounts were written-off without authorization or support.**

The utility clerk began this scheme by writing-off customer account balances without authorization or approval after funds were stolen.

There were no supporting documents for these unauthorized transactions.

(2) **Accounting records were then falsified to conceal additional losses of funds.**

All cash receipt transactions were first processed on a Quadrant cash register system.

At the end of the business day, these transactions were interfaced with the Eden utility accounts receivable system which marked all customer's accounts "paid".

The utility clerk then reversed the initial transactions from Quadrant and re-entered **only** customer's accounts paid by check. The Quadrant system total report reflecting this reduced amount of revenue was then attached to and agreed with the bank-validated deposit slip. The funds from transactions paid in cash were simply stolen.

DANGER: The Quadrant cash register total reports for each business day were attached to bank-validated deposit slips, making it easy to verify the information in a cash receipts test without going any further. However, while these two records were in agreement for the amount of revenue recorded each day and could be quickly reviewed, these amounts **did not agree** with the customer credits reflected in the Eden utility accounts receivable system (stand alone system). **Thus, the correct audit test to detect this irregularity must be to compare the amount of customer credits in the Eden system to the amount of revenue shown on a bank-validated deposit slip (and Quadrant system reports).**

To eliminate the audit trail, computer records for the prior transaction postings were deleted from the system, and hard-copy reports were destroyed. These changes were posted at unusual times of the day, and bank deposits were delayed until computer records had been altered.

There was little or no currency in the city's bank deposits.

Internal Control Weaknesses (Red Flags).

Segregation of duties problem. The utility clerk performed all tasks, including billing, collecting, depositing, posting and adjusting accounts, preparing accounting reports from computer systems, and handling customer feedback. Her supervisor was not very knowledgeable about the city's computer systems, and there was no oversight or monitoring of the utility clerk's work.

No one reconciled the Quadrant cash register system with the Eden utility accounts receivable system, and no one noticed that computer accounting records had been destroyed (after records were altered).

Cash collections from multiple cashiers were commingled into one cash drawer.

Computer passwords were not properly used. The first cashier reporting for duty signed-on the computer with their password. All other cashiers then simply recorded transactions on the system throughout the day. As a result, all transactions were recorded in the system as if they were processed by only one cashier (the one who signed-on). Operators are not identified in the data base with the transactions they processed.

The utility clerk took multiple payroll draws throughout the month.

Creditors frequently contacted the utility clerk at work about paying her debts.

The city received many utility customer complaints over several months regarding the timeliness of account postings and delays in depositing checks.

City employees noticed that the amount of "closing" cash from one day did not equal the amount of "opening" cash on the next day, and there often was not enough currency in the cash drawer to make change for customers.

Critical Audit Steps To Detect This Fraud.

Internal controls. In accounts receivable systems, review the separation of duties between the billing and posting/adjusting functions and the cashiering and depositing functions. Customer feedback must be reported to and resolved by an independent party, such as a customer service unit.

Analytical procedures. Review utility revenue for unusual fluctuations (declines).

Currency in bank deposits. Review composition records (is there any?). This has been a common element in almost every utility cash receipting fraud case in recent memory. Therefore, this is a "**must do**" audit step.

Account adjustments or write-offs. Determine whether all negative cash transactions (cancellations and adjustments) are authorized, approved, and properly supported.

Utility credits to customer accounts must agree with the bank-validated deposit slip amounts. Agree cash receipt totals from the Quadrant cash register system and bank-validated deposit slips with total customer credits in the Eden utility accounts receivable system for a specified period of time.

RISK ALERT -- UNNUMBERED CASH RECEIPT FORMS

1. The Fraud. **Skimming** of cash receipts is the fraud scheme of choice when cashiers operate in an environment where they collect funds from customers for services rendered. These frauds occur in at least two ways:

> (a) In some instances, cash receipt forms or other accountability records, such as cash registers, are not prepared by cashiers at the time funds are received. Funds collected are simply stolen.
>
> (b) When unnumbered cash receipt forms are prepared by cashiers, these forms may be the **only** documents which establish accountability for funds. After the customer departs, the cashier steals these funds and destroys the copy of the document which was prepared to record accountability for the transaction.

Unless there is some other type of **alternative record** within the entity to prove either of the above transactions actually occurred, no one will be able to determine the amount of loss if and when irregularities are somehow detected. If no alternative record exists, cashiers can easily **skim** money from the entity without detection.

2. The Problem (Risk). **When cash receipt forms are not prenumbered and controlled, neither managers nor auditors can establish the universe of all cash receipt forms issued or a cashier's total accountability for funds collected. This is an automatic "red flag" and internal control weakness**. This is why we always recommend entity managers: (a) prenumber original source documents for all types of revenue, maintain records of the form numbers issued to each cash receipting location, and then monitor the sequential use of all forms after issue; and, (b) record the number of prenumbered cash receipt forms issued on daily activity reports for control and monitoring purposes.

3. Detection. We found several unnumbered cash receipt forms during the previous audit of a health district and issued an internal control finding recommending management prenumber all such forms for accountability and control purposes in the future. While performing follow-up work during the current audit of the district, we found two cash receipt forms which had still not been prenumbered. The result of our substantive audit testing related to these two forms follows:

> (a) A $1,500 fraud case was detected in revenue associated with a "water testing" form. However, it was not detected by reviewing the accountability for these unnumbered cash receipt forms. In fact, this determination is usually not possible (see the results of our review of the second unnumbered cash receipt form discussed below). In this case, sufficient records did exist for us to trace transactions from these "water testing" forms to another cash receipting system where the transactions were subsequently recorded on a prenumbered cash receipt form and then processed on a cash register. Normally, these redundant cash receipting systems do not exist.
>
> This fraud was detected by reviewing "void" transactions on the cash register. The cashier who performed the closing and balancing actions processed fictitious "void"

transactions to eliminate accountability for funds just prior to recording the "Z" tape information for the day. After the prenumbered cash receipt form for the affected transaction was destroyed, the individual made the bank deposit in an amount which agreed with the reduced accountability for funds. Managers did not notice that one employee had processed 22 fictitious transactions in this manner over a two year period. These voided transactions involved a variety of revenue sources at the district. Since the employee performed the closing and balancing function only once a week, the district experienced a revenue loss on one out of every four days the employee performed this task (25%). The loss in this case would undoubtedly have been much greater had this employee performed this task on a daily basis.

(b) Our tests were inconclusive for revenue associated with a "food and beverage service worker's health record" form printed by the State of Washington Department of Health and issued to every health district in the state. This unnumbered, two-part perforated, blue form (index card size) is issued to food handlers who pass a health district test. It acts as a permit and must be possessed by every individual who works in a restaurant or similar food related activity. The district also printed a similar form for this purpose which was prenumbered for control purposes; however, **employees used both types of cash receipt forms to issue permits to the general public**. We compared records for completed tests to the data base for all permits issued during a specific period of time and found that the data base was inaccurate and unreliable for either management or audit purposes. Various numbering systems were used to record permits, sequential form numbers were missing, numbers were issued more than once, and names recorded in the data base did not agree with records of tests taken or permits issued. As a result of these irregularities, no one was able to determine whether all funds collected were properly recorded in the district's accounting system or deposited in the bank. Our current audit report will include a finding on this area of district operations.

The result of our audit of the "food and beverage service worker's health record" form at this health district matches my expectation for the results of our audits of most, if not all, of the entities who use unnumbered cash receipt forms (i.e.; inconclusive results). We need to identify this system deficiency as soon as possible to ensure entity revenue is properly safeguarded.

STATEWIDE AUDIT RISKS:

(a) Local Governments. Since this unnumbered state form may be used throughout the state, **local government audit teams** should consider including a review of the revenue generated through the use of this form in their next regularly scheduled audit of all health districts. The purpose of this review would be to determine whether a risk of loss exists for revenue received from the issuance of food handler cards.

(b) State Agencies. **Team SS** should also consider reviewing the use of these forms in their next audit of the State of Washington Department of Health. Since individual health districts appear to use their own food handler forms, we should determine whether these unnumbered state forms are still needed. If they are, they should be prenumbered and controlled. If they aren't, they should be discontinued. We should also determine if the

forms are used to record cash receipts within the department. The purpose of this review would be to determine whether a risk of loss exists for revenue received from the issuance of unnumbered food handler cards at the department similar to the situation described above for this health district.

4. Audit Steps to Detect Similar Fraud Schemes.

REMINDER: The audit steps listed below are not mandatory during audits of state agencies and local governments. You should consider performing one or more of these audit steps based upon you assessment of the risk that a loss of revenue might occur from the issuance of unnumbered cash receipt forms.

(a) Discuss the cash receipting system and internal control structure with management officials. Determine whether unnumbered cash receipt forms exist, and identify revenue streams at risk. If cash receipt forms need to be reprinted or redesigned, we should assist managers with this task. Ensure all cash receipt forms are prenumbered and controlled in future accounting periods. Identity any alternative records which might help establish the universe of all transactions. If possible, determine the universe of forms issued, and agree cash receipt totals to bank deposits and revenue recorded in the accounting system. **SPECIAL NOTE**: One problem you may encounter is that even if some types of forms are prenumbered, many of them may never be returned to the entity because customers change their minds or lose them. We found this condition in a previous DSHS fraud case involving fictitious disbursements for client services rendered by a vendor who was also a caseworker. There will always be problems trying to control this type of form. In such cases, we have to accept the fact that the number of documents on file is all that we have for audit purposes, and that the universe of actual transactions may never be determined.

(b) Perform analytical review procedures for revenue streams associated with unnumbered cash receipt forms. Search for missing revenue streams, and obtain explanations for unexpected declines in revenue from known revenue sources. Use professional skepticism when determining if you have received the correct explanation from management officials for missing or declining revenue. Perform substantive testing, as required, to verify any explanations received.

(c) Determine if the related service can be rendered without a payment being made, and whether the entity has received complaints from customers about non-receipt of the service they paid for and expected. Ensure customer feedback is resolved by an independent party or customer service unit.

(d) Determine whether all "void" transactions are properly authorized, approved by a supervisor, and supported by appropriate documentation. **Remember: A missing or falsified (altered) document is at the heart of every fraud.**

RISK ALERT -- NON-PUBLIC FUND CHECKING ACCOUNTS

1. The Fraud. A recent money laundering case in a school district emphasized the importance of knowing about the existence of checking accounts for non-public funds during routine audits. In this case, an employee stole entity miscellaneous revenue checks over a five year period and deposited them into checking accounts she controlled for both public funds and non-public funds. As the custodian of the advance travel fund ($55,000 in losses) and an employee association fund ($133,000 in losses), she then issued checks to herself, "cash", credit card companies, and other businesses for her own personal benefit. Her work was not properly monitored or supervised by entity officials.

This isn't the first time we've dealt with this type of fraud, nor the last. One other such case involved a housing authority where an individual used an employee "sunshine fund" for money laundering purposes. The custodian deposited entity revenue checks into the employee checking account and wrote checks to "cash" or to herself. While endorsements on the revenue checks were irregular, they were sufficient to be processed through the banking system.

2. The Problem (Risk). While our current and permanent audit files tell us about the existence and location of all checking accounts for public funds within the entity, **this is not necessarily true for checking accounts involving non-public funds**. Since these accounts are controlled by employees who are covered by the entity's personnel dishonesty bonding policy, both auditors and managers **may** have a need to know about the existence of checking accounts for non-public funds under certain circumstances. Of course, the risk is that employees will use these non-public checking accounts for money laundering purposes just the same as they do for public fund accounts. The ultimate question is whether management officials realize this risk and appropriately deal with it by having an independent party receive the monthly statement directly from the bank for all bank accounts, and by ensuring they reconcile them promptly and properly.

The State Auditor's Office has the authority to review checking accounts for public funds during all audits. In addition, if we have an indication or some other reasonable cause to believe that public funds have been processed through other than public bank accounts, we have the authority to follow the money where ever it goes.

3. Detection. We detected the advance travel fund portion of this fraud during a routine audit while reviewing endorsements on canceled checks. We subpoenaed the employee's bank records because she deposited almost all of the checks into her own personal bank account. Our review of these personal banking records then detected similar deposits from the employee association checking account. This led to the discovery of the remainder of the losses in this case. **NOTE**: If the employee had used only the checking account for non-public funds to perpetrate this fraud, the primary detection step available to us would have been **analytical review procedures** for miscellaneous revenue streams.

4. Audit Steps to Detect Similar Fraud Schemes.

REMINDER: The audit steps listed below are not mandatory during audits of state agencies and local governments. You should consider performing one or more of these audit steps based upon you assessment of the risk that a loss of revenue might occur from money laundering activities associated with checking accounts for both public funds and non-public funds.

(a) Identify all checking accounts for both public funds and non-public funds which are controlled by entity personnel. When deemed appropriate, review them for money laundering activities to address the risk that employees may have been misappropriated public funds. In these cases, we might only need to briefly review the bank records for non-public checking accounts (not audit them, per se) to assure ourselves that money laundering activities are not present.

(b) Review check endorsements for irregularities, and identify instances where the custodian's name or an irregular endorsement name is shown (i.e.; checks made payable to "cash" or for a personal expense).

(c) Test transactions from checking accounts for public funds to ensure that all disbursements are properly authorized and supported. Review deposit frequencies and amounts to identify potential irregular transactions.

(d) Review the segregation of duties for custodians of all checking account (i.e.; both public funds and non-public funds). Ensure the monthly bank reconciliation is promptly and properly performed by an independent party. Bank statements should be mailed directly to the person performing the bank reconciliation rather than to the fund custodian.

(e) Perform analytical review procedures for miscellaneous revenue streams. Search for missing revenue streams, and obtain explanations for unexpected declines in revenue from known revenue sources. Use professional skepticism when determining if you have received the correct explanation from management officials for missing or declining revenue. Perform substantive testing, as required, to verify any explanations received.

(f) Test the entity's procedures for controlling checks which arrive through the mail. Ideally, two people should open the mail, make a list of the transactions, and reconcile revenue totals to subsequent bank deposits using a **bank-validated deposit slip**.

(g) Review check voiding procedures for propriety to ensure these documents are properly safeguarded. If not available for review (i.e.; prematurely destroyed), determine whether these voided checks were actually issued and have cleared the bank.

5. Reminder About Methods Used to Launder Entity Revenue and Disbursement Checks.

(a) Perpetrators launder negotiable instruments **inside** the organization by:

(1) Using a check for cash substitution scheme in the organization's daily bank deposit.

(2) Making irregular deposits into and subsequent withdrawals from an authorized bank account with a name similar to the name of the organization, **such as an employee fund**.

(3) Making irregular deposits into and subsequent withdrawals from an authorized bank account used within the organization (i.e.; general depository, imprest, trust, etc.).

(4) Making a "cash-back" withdrawal from a deposit for any type of bank account at the organization.

(5) Altering checks by increasing the amount and removing an equivalent amount of currency from the till drawer and subsequent daily bank deposit.

(b) Perpetrators launder negotiable instruments **outside** the organization by:

(1) Making deposits into a "bogus" bank account in the name of the organization.

(2) Making deposits into their own personal bank or credit union account.

(3) Cashing the checks at a financial institution or business/vendor.

RISK ALERT -- BOGUS CHECKS AND CHECK FRAUD

Check fraud by individuals outside the government is increasing. It will continue to get worse. Nationally recognized experts say that the recent growth in check fraud has reached epidemic proportions. No company, municipality, or financial institution is immune. The Office of the Comptroller of the Currency estimates that check fraud losses in 1996 exceeded $12 billion, up from $5 billion in 1993. More than 1.2 million worthless checks enter the banking system each day. The number of cases involving fraudulent checks of $100,000 and higher during 1990-96 increased 300%. This is cause for alarm.

How are we affected by this wave of crime? There have been a number of "check production mills" operating in the Puget Sound region in recent years. Until now, governments had not been affected. But, that has all been changed, with three governments being hit recently -- a school district, a county, and a hospital.

Check production mills produce bogus checks using a computer and check stock paper obtained from any office supply store. A significant investment is not required to perpetrate this crime. They hire individuals to cash the checks at various financial institutions and then move to another city before the police have an opportunity to catch them. Here's what they do.

> First, these mills steal mail from post office boxes and individual mail boxes, predominately in rural areas. They can also obtain this same information from businesses and governments who throw away their trash rather than use paper shredders to dispose of sensitive financial records. They steal the trash by "dumpster diving". Obtaining the mail or trash gives the fraudsters the key item of information needed to perpetrate the crime -- the bank account identification number of a checking account, whether that be personal, business, or government. Businesses and governments are frequently targets in these schemes because the fraudsters are able to issue checks in large amounts without becoming suspicious to a bank teller.
>
> Second, they use their computer and check stock paper to produce phony checks on the bank accounts they have identified.
>
> Third, they hire people to cash these bogus checks. They obtain false identification for these individuals which matches the payee name listed on the bogus checks. These individuals are paid a percentage of the amount of the checks they are able to cash. These checks are normally cashed at financial institutions.
>
> Finally, when they feel that the market has been saturated, they close-up shop and relocate to another city. They then begin the process all over again.

There are two basic ways to detect this crime. The bogus checks are either detected by the bank or by the individual, business, or government when they perform their monthly bank reconciliation. If detected promptly, the banks suffer the ultimate loss in these cases. This is what happened in the three cases cited above. While the fraudsters use the checks of individuals, businesses, and governments in these schemes, banks are the true target. When investigators

asked a prominent criminal why he kept robbing banks, he replied: “Because that’s where the money is!” Check fraud is merely a variation on this theme.

What can the State Auditor’s Office do to assist the governments we audit to defend themselves against this crime? Here are a few tips.

(1) We should encourage governments to **shred all financial records before discarding them**. This includes bank statements.

(2) Governments should check with their financial institution to **make sure that their check stock meets all the requirements of the banking industry**. If this is done, banks readily accept the responsibility for fraudulent checks because they feel that the organization has done all that it can do to prevent check fraud. Of course, no system, feature, or program can completely eliminate check fraud. No prevention method is foolproof. However, specific practices can reduce exposure to check fraud by complicating the criminal’s task. **Using multiple check security features can thwart many types of check fraud**. This encourages criminals to seek easier targets and avoid organizations whose checks make replication more difficult. **Using selected bank services, such as Positive Pay, in combination with highly secure checks can virtually eliminate an organization’s financial exposure to check fraud**.

(3) We should encourage governments to **establish tight controls over the storage and distribution of check stock**. This is essential in preventing the theft and unauthorized use of government checks. Check stock must be kept in a secure, locked area with access restricted to only those persons responsible for issuing checks. Only these people should have keys or combinations to the locked storage area. **Locks or combinations should be changed** when employees terminate employment with the government and at least annually to ensure they have not been compromised. **Safe and vault combinations should not be written-down anywhere**. Check issuance procedures should ensure that all check stock is accounted for and controlled during processing.

(4) **Bank account reconciliations should be performed as soon as the bank statement arrives, but not later than 30 days after it has been prepared by the bank**. All suspicious checks should be reported to the organization’s financial institution immediately. If fraudulent transactions are noted during the first 30 days, banks readily accept their responsibility for them. Thus, they suffer the loss, not the government. If not detected during this time period, the government ends up accepting the bank’s liability as their own, certainly not a desirable condition. **This is the single most important reason we can provide to government to encourage them to perform monthly bank reconciliations in a timely manner**. This reconciliation should also be **performed by a person who is independent of the account custodian**. And, this independent party must receive the unopened bank statement directly from the financial institution. **One of the first steps to be performed during the bank reconciliation process is to determine whether any “bogus” checks have been redeemed by the bank. Of particular interest are checks that have not been issued by the organization (such as those issued by “check production mills” outside the government), and duplicate or voided checks which clear the bank (schemes by employees inside the government)**.

(5) We should advise governments to make sure that the signatures of executive officers are not included in annual financial reports or other public documents. **These signatures can be easily forged by using optical scanners**.

(6) We should advise governments to make sure that they establish maximum dollar parameters for their disbursement accounts so that forged or altered checks exceeding that amount will be rejected by the bank. **Do not print the maximum allowable dollar limit on the face of the check because the fraudster will create checks for amounts just below the authorized limit**.

(7) We should advise governments to open a separate bank account to be used exclusively for incoming wire transfers. **Fraudsters obtain accurate account information by posing as customers requesting wiring instructions**.

There are many more internal controls in the area of check security. But, these are the major items of interest relating to check fraud described in this risk alert. Share this document with the entities you audit. They will appreciate the information. And, incorporate these types of questions in the audits you perform in government treasury functions.

RISK ALERT -- DESTRUCTION OF ORIGINAL SOURCE DOCUMENTS

There have been a number of inquiries recently concerning public entities that destroy original source documents after receipt. Each case has involved utility billing stubs in cities; however, this condition could also occur in the cash receipting function of any state or local government. Recent cases have been as follows:

(a) Case number one. Customers used bank "PAY-ON-LINE" services to make their utility payments to a city using a personal computer at their home. Customers using this bank service are able to pay all their bills in this manner. After notification of the transaction, the bank deducts the payment amount from the customer's bank account. PAY-ON-LINE then sends a remittance advice to the city along with the individual customer checks created using this on-line banking service. The remittance advice includes the detail of each transaction, such as the customer's name, address, account number, amount, and any other descriptive information needed to process the transaction.

(b) Case Number Two. Customers used a service company to make their utility payments to the city. The service company then sends a remittance advice to the city along with a single check for the total amount due for all customers listed on the document. The remittance advice includes the same type of detail as indicated in case number one above.

In both of these cases, utility billing stubs were mailed to customers notifying them of the amount due to the city; however, they were never returned. Thus, the remittance advice becomes the original source document for these cash receipt transactions. It indicates the total amount paid to the city by each customer as well as the mode of payment of the transaction. **In both of these cases, the city prepared manual utility billing stubs for each customer and then destroyed the remittance advice for the transactions**. Preparing manual utility billing stubs can be a redundant and unnecessary step. But, if the city wishes to prepare this duplicate document, they must also retain the remittance advice on file with the batch of utility billing stubs supporting the daily bank deposit.

Both of the above types of payments were recently encountered in an accounts receivable operation at a school district day care program. This included individual customer payments like case number one above, and collection agency payments similar to case number two above. In the future, we're going to be seeing more and more of this type transaction throughout government as the general public becomes more computer literate.

(c) Case number three. Customers made utility payments at another city in two ways. When customers made payments over-the-counter, the city prepared an official, prenumbered receipt to record the payment and then **destroyed the utility billing stub**. When customers made payments through the mail or by using a drop box, the city prepared a log listing the payments and **destroyed the utility billing stubs**. The payment log listed the date, customer's name, account number, and mode of payment of the transactions. At the end of the day, all over-the-counter payments were also recorded

on the payment log. The log was then used to balance to total cash receipts on-hand, prepare the daily bank deposit, and post the customer's accounts "paid".

In this case, destroying the utility billing stubs is an unnecessary step, while preparing the payment log is a redundant step. But, if the city wishes to prepare this duplicate document, they must retain the batch of utility billing stubs on file to support both the daily bank deposit and the customer account posting report. As a reminder, **the payment log in this case is a "summary level" document** which provides little or no value in determining the completeness of cash receipts.

Audit Risk. Destruction of original source documents (i.e.; remittance advices and billing stubs) is definitely a "red flag". You can easily see that a utility accounts receivable clerk or cashier could disregard the original information received and **record payments for any customer they choose within the system**. Destroying the remittance advices and utility billing stubs would conceal this action and blur the audit trail. Therefore, there is a risk for fraud. Fraudsters could easily perpetrate a lapping scheme under these circumstances.

Some tips to help you identify the destruction of public records follow.

Review batches of utility billing stubs for manually prepared documents. From a discussion with entity staff, determine why this step was necessary.

Inquire of entity staff about sources of customer payments and methods of payment currently in use. If PAY-ON-LINE bank services, payment service providers, and collection agencies are used, there should be remittance advices present for these payments. Search for them during cash receipts testing.

Rely on your experience and knowledge of similar entities to identify missing source documents. You must be inquisitive. Determine why documents that should be present have not been found within the entity.

Trial Preparation

PRE-DEPOSITION INFORMATION

The purpose of these instructions is to inform you what a deposition is, why it is being taken, how it will be taken, and pitfalls to avoid during its taking.

1. What is a deposition?

A deposition is your testimony under oath. You will be asked questions by the opposing attorney and in some cases, perhaps, the prosecuting attorney, and the questions and your answers will be recorded by an official court reporter. There will be no judge present. The only difference between testimony at a deposition and testimony in the courtroom is that there is no judge presiding and ruling over the matters as they arise. The judge may rule later, however, should some dispute arise over the admissibility at trial of your deposition testimony.

2. The purposes of a deposition.

The opposing side is taking your deposition for three reasons. The first reason is that they want to find out what facts you know regarding the issues in the law suit. In other words, they are interested in what your story is now and what it is going to be at the trial. Secondly, they want to pin you down to a specific story so that you will have to tell the same story at the trial. From your deposition testimony, they will know in advance what your testimony at trial will be. Thirdly, they hope to catch you in a lie because if they do catch you in a lie, they can show at the trial that you are not a truthful person and, therefore, your testimony should not be believed, particularly on the crucial points.

These are very legitimate purposes and the opposing side has every right to take your discovery deposition for these purposes and in this fashion. Correspondingly, you have the same right to take the discovery deposition of the opposing litigant.

3. Pitfalls to avoid.

Always remember that either as a litigant or a witness you have no purpose to serve other than to give the facts as you know them. You must give the facts if you have them. You do not, however, have to give opinions and, therefore, you should not give opinions. Generally speaking, if you are asked a question calling for an opinion, I will object to the question. After my objection, however, if I advise you to go ahead and answer and you do have an opinion on the subject, you may give it.

Never state facts you don't know. Quite frequently you will be asked a question by an attorney and in spite of the fact that you feel that you should know the answer, you do not and, therefore, you will be tempted to guess or estimate what the answer should be. This is a mistake. If you do not know an answer to a question, even though you would appear ignorant or evasive by stating that you don't know, you should, nevertheless, do so because a guess or an estimate for an answer is almost always the wrong answer and one from which the opponent can show that you either don't know what you are talking about or imply that you are deliberately misstating the truth. Generally speaking, the opposing attorney is in a position to know what your answer

should have been, and it may very well be that the reason he asked the question was because he knew you wouldn't know the answer, but felt that you would be compelled to guess. Remember, the deposition is not a quiz. You should combat your natural inclination to provide answers when, in fact, you don't actually know the information sought.

Never attempt to explain or justify your answer. You are there to give the facts as you know them. You are not supposed to apologize or attempt to justify those facts. Any attempt to do so would make it appear as if you doubt the accuracy or authenticity of your testimony.

You are obligated to give only the information you have readily at hand. If you do not know certain information, do not give it. Do not turn to the prosecuting attorney or anyone else and ask for the information, or do not turn to another witness, if one should be present, and ask him or her for the information. Do not promise to get information that you don't have readily at hand unless the prosecuting attorney advises it. If you know an answer to a question at the time that it is being asked, then you should answer it. Do not agree to look anything up in the future and then supplement the answer you are then giving unless the prosecuting attorney advises you to do so.

Do not, without the prosecuting attorney's request, reach into your pocket for a Social Security card or other documents. A discovery deposition is to elicit facts you know and have in your mind and is not for the production of documents. If the opposing side is interested in obtaining documents from you, they may employ proper legal procedures to obtain them. Do not ask the prosecuting attorney to produce anything in his file at the time, because the same rule for obtaining such documents applies to those matters that applies to things that may be in your pocket.

Do not let the opposing attorney make you angry or excited. Loss of composure may cause you to say things that may be used to your disadvantage later. It is sometimes the intent of attorneys to get a deponent excited during his testimony hoping he will say things that may be used against him. Under no circumstances should you argue with the opposing attorney. Give him only the information you have; that is all he is entitled to. The mere fact that you become emotional about a point could be to your opponent's advantage.

If the prosecuting attorney begins to speak, stop whatever answer you may be giving and allow him to make his statement. If the prosecuting attorney is making any objection to the question that is being asked of you, do not answer the question until after he has made his objection and advises you to go ahead and complete your answer. If the prosecuting attorney tells you not to answer a question, then you should refuse to do so.

You may take your time in answering a question. Remember, the deposition transcript does not show the length of time you used in considering your answer. It is advisable, however, to answer all questions in a direct and forthright manner. The most important thing to remember is that if you don't know an answer to a question, say so.

Tell the truth. The truth in a deposition will never really hurt you. The prosecuting attorney may be able to explain away the truth, but there is no convincing explanation of why a client lied or concealed the truth.

Never joke in the deposition. The humor would not be apparent in the cold transcript and may make you look crude or cavalier about the truth.

Do not volunteer any facts not requested by a question. Why make things any easier for the opposition? Sometimes the person asking the questions may pause in an effort to get you to expand upon your answer. Resist the temptation to do so. Answer directly and wait for the next question.

After the deposition is over, do not chat with the opponents or their attorney. Remember, the other attorney is your legal enemy. Do not let his friendly manner cause you to drop your guard and become chatty.

After you have read all of these suggestions, please note any questions you may have and ask them of the prosecuting attorney prior to the deposition.

POINTERS FOR A WITNESS

1. Be absolutely honest. The beauty of telling the truth is that you do not have to remember what you said.

2. Know exactly what you are going to testify to and don't guess about something you don't know. If you don't know, say so.

3. Make certain you understand the question before answering it. If you don't understand the question, ask the attorney what he means. Keep your answers simple and to the point.

4. Take your time in answering. Think about the question, then about your answer and give it straight to the point. Answer slowly and you will be asked questions slowly.

5. Answer only the question that is being asked, then stop. Don't volunteer anything that is not asked for. If the question can be answered "yes" or "no", answer it that way. Then, if you want to explain, do so. Remember, you can always explain any answer to make certain that the attorney understood your answer.

6. If there is any objection by either attorney, stop talking.

7. Give an audible answer so that all can hear. Speak loudly and clearly. Don't just nod or shake your head.

8. Don't look to the attorney for help during cross-examination or for his approval or disapproval after answering a question. Look at the jury or at the questioner; otherwise you will create a bad impression.

9. Beware of questions involving distance and time. Don't guess. If you don't know, say so. Don't say "a minute" when you mean "a second". If you make an estimate, make sure everyone understands you are only estimating.

10. Don't fence or argue with the attorney on the other side. Remember, you are a witness and not an advocate. The attorney has every right to cross-examine you and if you lose your temper, get evasive, or make smart talk, you may be reprimanded by the judge.

11. Don't lose your temper no matter how hard you are pressed. Just stick to your story and tell the truth.

12. Be courteous. Answer "yes, Sir" or "no, Sir." Be polite and you will make a good impression on the court and the jury.

13. Be sure to admit freely that you have talked to the attorney on either or both sides of the case or to the investigators on both sides, if you are specifically asked. There is nothing wrong in having discussed the case with those concerned before you testify, but don't mention the word "Insurance" before the jury in any respects because it tells the jury there is "insurance" and may result in influencing them or in a mistrial (which means going all through the case again).

14. Look the jury in the eye when you tell your story. Sit up straight. Keep your hands from your face and from other objects. Don't chew gum. Don't smoke in the presence of jurors during recess. Remember, the jurors are naturally sympathetic to the witness and want to hear what you have to say.

15. Steer clear of jurors during recess. Under no circumstances should you approach a juror, even though it may be on a matter wholly foreign to the case on trial. This will avoid suspicion.

16. Dress neatly and wear conservative clothes.

17. Remember that being a witness is the performance of a civic duty, equally as important as serving on a jury, and is of the utmost importance in the preservation of our system of justice.

PROFESSIONAL STANDARDS BULLETIN NO. 87-4

SOURCE: THE INTERNAL AUDITOR/JUNE 1987

Professional Proficiency - Expert Witness Testimony

Question: In communicating the results of audit work, as described in Standard 430, it is possible that an auditor would be requested to testify in court as an expert witness. Please provide some suggestions about how an auditor should prepare for testifying as an expert witness.

Answer: Testifying in court as an expert witness can involve communicating results as discussed in Specific Standard 430, but also involves issues such as due professional care (Specific Standard 280) and an auditor's knowledge, skills, and disciplines (Specific Standard 250).

Before appearing as a witness, it is advisable to consult with an attorney who can inform the auditor as to what the nature, scope, and strategy of the trial are and how the expert testimony provided by the internal auditor fits into the resolution of the matter before the court. In addition, internal auditors need to inform the appropriate members of their organization's management about court appearances. Adequate preparatory work should be done prior to appearing as a witness; this includes studying prior briefs, testimony, decisions, and documentation. The following suggestions are provided as additional guidance.

Anticipate questions and attorneys' lines of reasoning. It is advisable to formulate answers in advance for questions that you expect will be asked. A mock trial exercise can also be helpful in identifying weak areas of testimony.

Provide counsel with information to develop your testimony. Specific questions should be developed in advance to ensure that your testimony is as useful as possible.

Review workpapers or exhibits. Study exhibits and other documents presented to you as long as necessary to understand them. Do not jump to conclusions because the documents may not be what they appear to be. As audit workpapers are prepared, it is equally important that they fully support the conclusions reached.

Understand questions before answering. Witnesses are not required to, nor should they, answer any question that is not fully understood. Request rephrasing or clarification until the question is understood. Do not be led into saying something that isn't meant. Avoid quick answers to leading or overly simplistic questions.

Do not guess. It is acceptable for the witness to state "I don't know." Do not speculate in order to answer the question.

Answer only the question asked. Do not volunteer information or elaborate on answers. Answers should stay well within the scope of the question.

When asked if you agree with statements from a previous witness, be specific. If you agree or disagree in part and the attorney will not allow you to explain, state that you can't answer the question.

Do not denigrate opposing witnesses. When disagreeing, attempt to cite authoritative support.

Correct errors in testimony. If you become aware of errors in previous testimony given by you, correct it as soon as possible. This can be accomplished by stating that an item, which was discussed previously, needs to be corrected. Correct it, and explain at that time why the mistake occurred.

Listen to lawyer's objections. If a lawyer objects to a question, do not answer it until the lawyer has completed the objection. In a deposition, follow the advice of your attorney. At trial, wait to answer until the judge rules on the objection. If in doubt, ask the judge.

Tell the truth. The value of an expert witness is the knowledge and experience that can be provided to solve the dispute at hand. Speak loudly and clearly in delivering answers.

Present facts versus feelings or unsupported opinions. It is not the witness's responsibility to advocate a party's position in a lawsuit. Testimony should be given in a manner which is free of bias or the appearance of favoritism. Don't quibble or be evasive.

Be yourself. Do not play a role. Being yourself will make it easier to think and answer questions. An expert witness should avoid the appearance of arrogance as this will diminish the value of his or her testimony in the opinion of the judge or jury.

Dress conservatively. An expert witness's testimony will be more believable if the person is dressed neatly and professionally.

Avoid joking or sarcastic remarks. Be courteous and polite to everyone in the courtroom. Jokes and sarcasm rely on eye contact and facial gestures to convey their meaning, and these are missing from written depositions and court transcripts.

Do not lose your temper or become argumentative. Each answer should be given only after careful reflection of the question. Avoid anger or fatigue by requesting a short break.

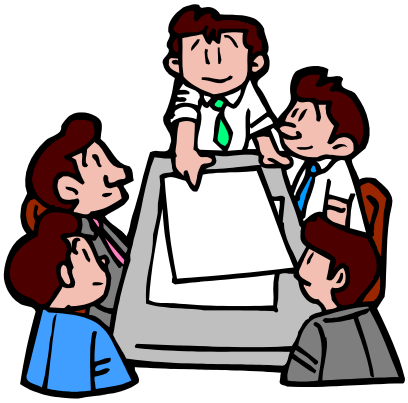
Avoid the use of jargon or technical terms which may confuse the jury or judge. Take extra care to present testimony that is understandable to the layman. Become familiar with courtroom facilities which will be needed if more than oral testimony is used (i.e.; blackboard, slides).

Do not look at your lawyer. This can be mistaken as direction from your attorney. Short answers should be directed to the lawyer asking the question; longer answers should be directed to the jury, particularly members who appear receptive. Do not force eye contact on a member of the jury who avoids it.

Do not talk with members of the jury. It is inappropriate for a witness to converse with a member of the jury. If this occurs, politely state that the court has instructed you not to converse with them. If this action persists, inform the lawyer who arranged for your appearance. Be very cautions in discussing the status or strategy of the trial outside the courtroom since conversations can be overheard in the most unsuspecting places.

These bulletins are prepared for information only by a subcommittee of the Institute of Internal Auditor's Professional Standards and Responsibilities Committee. For additional guidance, readers should refer to the Standards. Any questions regarding the application of The Institute's standards pronouncements should be directed to Marjo Miller, Transok, Inc., P. O. Box 3008, Tulsa, Oklahoma 74101.

Interviewing Fraud Suspects



TIPS ON INTERVIEWING FRAUD SUSPECTS

A successful interview of a fraud suspect is critical in fraud development. Conducting such interviews is not an easy assignment as it is far easier to fail than to succeed. The ideal situation is to have an auditor who is not only trained and experienced in interviewing, but also has the personality characteristics necessary to deal with the stress and challenges associated with such interviews.

The following are proven tips resulting from numerous successful interviews:

1. The interview needs to be planned with clear objectives in mind.

2. The interviewer needs to understand the mechanics of the fraud.

3. The interviewer should know the answers to all questions, and the questions should have a logical sequence.

4. The interview should be conducted in a private setting with no distractions.

5. The interviewer needs to be confident and maintain a positive attitude.

6. Give the suspect the minimum advance notice of the interview.

7. Auditors do not have arrest authority and are not agents of those who do; so, **do not** give a Miranda Warning.

8. Initiate the interview in an unassuming manner and give the impression you are just trying to resolve some standard audit exceptions.

9. Do not tape the interview or take notes. Write up the interview from memory later.

10. The interviewer needs to maintain the initiative throughout the interview and be persistent.

11. A calm, professional, but relentless, questioning style is most effective.

12. Don't allow the suspect to succeed with obvious untruths and diversions. Don't accept "I don't know" as an answer to your questions.

13. Pin the suspect down to detail.

14. Present available physical evidence of a fraud at the most critical time.

15. Make it easy for the suspect to confess by using "positive" questions. Provide the suspect with good reasons to confess.

16. Eventually confront the suspect with their guilt. Telling the suspect you believe them responsible for a loss is not slanderous.

17. It is desirable, although not critical, to get the suspect to sign a statement to any admissions made.

CASE LAW BEARING ON AUDITS BY THE OFFICE OF STATE AUDITOR

(1) Miranda v. Arizona, 384 U.S. 436 (1966).

Supreme Court case. The employee must be informed of their rights (self-incrimination) before any interview is conducted.

Employees of the State Auditor's Office are not required to administer Miranda Warnings during interviews conducted with employees during the course of our audits because we do not have the power to arrest, and do not interview employees in a custody environment. See case on State of Washington v. Tina Marie Nelson below.

Auditors rarely, if ever, act as agents of a law enforcement agency. But, if this is the case, let the law enforcement agency give Miranda Warnings to the suspect.

(2) National Labor Relations Board v. J. Weingarten, 420 U.S. 251 (1975).

Analysis. A union employee is entitled to have a union representative, another employee, or any person of their choosing present during an interview if there is some expectation that a future disciplinary action may occur as a result of the interview, which is almost always the case. The employee has this right, but the employer does not have to inform the employee of this right prior to the interview. Most entities advise their employees of this right before the interview is conducted to ensure that they are not subsequently criticized for not doing everything possible to protect the employee's rights.

Supreme Court ruling, *National Labor Relations Board v. J. Weingarten*, 420 U.S. 251 (1975).

Case Summary: In Weingarten, the employer had called in an employee for questioning regarding allegations that she had taken money. During the course of the questioning, the employee several times asked the manager to call in the union shop steward or another union representative, and the manager refused to do so.

In Weingarten, the Supreme Court ruled that employees in unionized work forces are entitled to representation in investigatory interviews which the employee reasonably believes could result in disciplinary action.

The Court then went on to explain that this right to representation would arise only when an employee actually requests representation and only when the employee has a reasonable belief that the investigation will result in some sort of disciplinary action.

The Court held that an employer violated Section 8(a)(1) of the Act by denying an employee's request that a union representative be present at an investigatory interview which the employee reasonably believed might result in disciplinary action.

The Court also stated the following. The union representative whose participation the employee seeks is however safeguarding not only the particular employee's interest, but also the interests of the entire bargaining unit by exercising vigilance to make certain that the employer does not initiate or continue a practice of imposing punishment unjustly. Such a union representative is knowledgeable and experienced and has the ability to help both the individual employee and the employer as well as the ability to safeguard the interests of the entire bargaining unit.

These statements explain that the right to the presence of a representative is grounded in the rationale that the Act generally affords employees the opportunity to act together to address the issue of an employer's practice of imposing unjust punishment on employees.

Because the facts at issue in this case involved a request for the presence of a union representative, the Court's decision did not specifically refer to circumstances involving the request for a coworker representative in nonunion settings. The Board, however, has addressed this precise issue on several occasions.

In *Materials Research Corporation*, 262 NLRB 1010 (1982), the Board found **that the Weingarten right includes the right to request the presence of a coworker at an investigatory interview in a nonunion setting**. The Board found that the ability to avail oneself of this protection does not depend on whether the employees are represented by a union.

The Board overruled *Materials Research Corporation* in *Sears, Roebuck and Company*, 274 NLRB 230 (1985), and held that **Weingarten principles do not apply in circumstances where there is no certified or recognized union**. The Board also expressed the view that extending Weingarten rights to employees not represented by a union is inconsistent with the Act because it infringes upon an employer's right to deal with employees on an individual basis when no union is present.

The Board modified the *Sears, Roebuck and Company* rationale in *E.I. DuPont and Company*, 289 NLRB 627 (1988) when it adhered to its position **that Weingarten rights are not applicable in nonunion settings, but acknowledged that the statute might be amenable to other interpretations**.

The Board acknowledged that the Supreme Court's decision in Weingarten had referred only to union representatives but determined that that was due to the particular fact pattern under consideration there and not to any desire on the part of the Court to limit the right to such a session. Thus, nonunionized employees should be accorded the same right.

In *Epilepsy Foundation of Northeast Ohio*, 331 NLRB 92 (2000), Cases 8-CA-28169 and 8-CA-28264 (July 10, 2000), **the National Labor Relations Board disagreed with the prior Board's holding *in Sears, Roebuck and Company* and *E.I. DuPont and Company*, and finds that a return to the rule set forth in *Materials Research***

***Corporation*, i.e., that Weingarten rights are applicable in the nonunionized workplace as well as the unionized workplace, is warranted**.

Case Summary: Borgs had reason to believe that he had been called to an investigatory interview that could result in disciplinary action. As a result, he made a timely request that Hasan be allowed to accompany him to the interview. Management denied this request, and Borgs was discharged because of his refusal to attend the interview. The Respondent contended that Borgs was not interrogated about or disciplined for discussing salary information with other employees who voluntarily disclosed such information, but for the unauthorized acquisition and disclosure of salary information concerning supervisory employees who had not disclosed it to him.

This rationale is equally applicable in circumstances where employees are not represented by a union, for in these circumstances the right to have a coworker present at an investigatory interview also greatly enhances the employees' opportunities to act in concert to address their concern "that the employer does not initiate or continue a practice of imposing punishment unjustly". In a dissenting argument by a member of the Board, it was stated that a mere coworker brings few if any of the qualities of a union representative to the table.

The Act clearly protects the right of employees – whether unionized or not – to act in concert for mutual aid or protection. Further, the right to have a coworker present at the investigatory interview affords unrepresented employees the opportunity to act in concert to prevent a practice of unjust punishment.

We also find that the concerns raised by the Board in *E.I. Dupont and Company* do not warrant allowing an employer to prohibit the exercise of Weingarten rights in nonunionized workplaces.

An employer is completely free to forego the investigatory interview and pursue other means of resolving the matter.

Employees are not obligated to request the presence of a Weingarten representative, and – as in the unionized workplace – can freely evaluate the strategic merits of any particular course of action in this regard.

Unrepresented employees may have an even greater need for support during an investigatory interview because they are without the safeguards of a collective-bargaining agreement, which checks an employer's ability to act in an unjust or arbitrary way, and without the protections afforded by a grievance-arbitration procedure. Thus, unrepresented employees should be able to look to coworkers for assistance during an invesgtigatory interview in order to counteract this imbalance of power between employers and unrepresented employees.

In sum, we hold that the rule enunciated in Weingarten applies to employees not represented by a union as well as to those that are. We overrule the Board's decision in *E.I. Dupont and Company* and return to the standard set forth in *Materials Research Corporation*. In addition, we also shall apply the rule enunciated

today to the facts of this case and find that the Respondent (*Epilepsy Foundation of Northeast Ohio)* violated Section 8(a)(1) of the Act by terminating Borgs for insisting on having his coworker, Hasan, present at an investigatory interview.

(3) Garrity v. New Jersey, 385 U.S. 483 (1967).

If an employee is compelled to answer questions under threat of losing their job should they refuse, any statements obtained are coerced and cannot be used in a subsequent criminal proceeding.

All interviews conducted by state auditors are strictly voluntary. If state or local government employees do not want to talk to us during an interview, we do not force them to do so.

(4) General Insurance Company v. Dyer, 7 Wn. App. 411, 499 P.2d 910 (1972).

Audit costs for rehabilitating the integrity of the entity's financial records in order to establish the amount of the loss are recoverable from bonding companies unless the bonding policy specifically has a clause which excludes the payment of audit costs.

(5) Superior Court of Washington for Cowlitz County, State of Washington v. Tina Marie Nelson, Case No. 94-1-00600-0, September 12, 1995 (1995).

Employees of the State Auditor's Office are not required to administer Miranda Warnings during interviews conducted with employees during the course of our audits because we do not have the power to arrest, and do not interview employees in a custody environment. This fact was established in a 3.5 Pre-Trial Hearing in the City of Longview fraud case involving funds misappropriated from building permit fees. A guilty verdict by jury trial was obtained in this case.

(6) Washington Supreme Court Case, State v. Warner, 125 Wn.2d 876, 889 P.2d 479 (1995).

The case applies to every interview conducted during fraud audits. The court concluded that any state employee conducting a "custodial interrogation" would probably qualify as a state agent and would need to use Miranda Warnings. Two conditions which apply are: (1) the power of arrest; and (2) custody.

> SAO does not have the power of arrest. But, we take great care to ensure we do not inadvertently become an agent of law enforcement officials during fraud audits. After meetings with these officials, we perform audit tests in our own right, not at their request (agent relationship never established). There are exceptions (City of Tacoma and Seattle School District cases are good examples). If an agency relationship is established during a fraud audit, let the law enforcement officials Mirandize the individual.
>
> SAO does not interview in a custodial situation. We take great care to ensure we do not inadvertently interview an individual in a "custodial" manner. The arrangement of the interview meeting room is critical.

The Fraud Specialist is a critical player in all interviews we conduct during fraud audits.

(7) Superior Court of Washington for Clark County, State of Washington v. Dennis William Watson, Case No. 96-1-00660-2, September 20, 1996 (1996).

This case resulted from a Clark College whistleblower investigation conducted by SAO.

The court concluded that SAO's Subpoena Duces Tecum (bring me the papers) cannot be used as a search warrant to seize records. Use of a subpoena was determined to be inappropriate because SAO acted as an agent of a law enforcement agency (Washington State Patrol) in the case. The Clark County Prosecuting Attorney's Office denied a request for a search warrant. SAO's subpoena was then used to obtain the evidence. Accordingly, all evidence gathered was determined to be inadmissible in court. Thus, the case was dismissed.

SAO must give the person or entity served by subpoena at least five days to produce the records.

INTERVIEW OUTLINE DOCUMENT

INTRODUCTION

1. The (Entity) has experienced a loss of funds from widget machine revenue during at least the period (Dates). We are interviewing all employees who were involved in the widget machine revenue system to determine whether any specific employees are involved. Are you willing to cooperate with the (Entity) and assist the State Auditor's Office in this investigation?

2. Employees of the State Auditor's Office are not required to administer Miranda Warnings during interviews conducted with employees during the course of our audits because we do not have the power to arrest, and do not interview employees in a custody environment. This fact was established in a 3.5 Pre-Trial Hearing during Cowlitz County Superior Court case number 94-1-00600-0 (State of Washington v. Tina Marie Nelson) on September 12, 1995. However, to ensure that there are no subsequent concerns raised in this case about your rights pertaining to Miranda Warnings and Weingarten Warnings, we want to make sure that you have been advised of and understand the following:

a. If you are a member of an employee bargaining unit that is represented by a union, you are entitled to have a union representative present during this interview.

(1) Are you represented by a union?

(2) If so, do you want to have a union representative present?

b. You are not required to discuss any information related to this investigation with us; however, your input is considered to be valuable and will assist the State Auditor's

Office in making recommendations to the (Entity) to improve internal controls over widget machine revenue in the future.

c. The door to this interview room has been closed for your privacy. It is not locked, and your exit from this room has not been obstructed in any way. You are free to leave this interview room at any time.

d. The time of this interview has been scheduled so that it does not conflict with your routine lunch period or quitting time. It is being conducted during (Entity) business hours, uses (Entity) accounting records, and is considered to be an extension of your normal work environment.

e. If you want to take a short break from this interview for any personal reason, you may do so at any time.

Do you understand your rights as I have explained them to you from the information we have covered up to this point in this interview?

Do you want to proceed?

BACKGROUND

1. Explain your job responsibilities and duties associated with the (Entity) widget machine revenue system.

a. Widget Sales Office.

(1) Access to widget machine key box and keys.

(2) Access to the widget ticket inventory.

(a) Destruction of unused (i.e.; voided, spoiled, etc.) widget tickets.

(3) Placing widget ticket stock in and removing money from widget machines.

(a) Routine daily activity.

(b) Emergency activity (i.e.; ticket jams, machine malfunctions, etc.).

(4) Transporting funds from the widget machines to the Widget Sales Office (unlocked bank bags).

(5) Access to cash receipts in the office.

(a) Ability to move or relocate the safe (not chained to floor).

(b) Safe combination.

1. Knowledge of safe combination.

2. Knowledge of where the safe combination was written down in the office (identify).

3. Frequency of safe combination change (i.e.; not in over 4 years).

(c) Cash receipts commingled for many days in the safe.

1. Unauthorized change fund (estimated amount).

(d) Making a comparative analysis of widget machine revenue from year to year and analyzing variances.

(e) Making change for other college offices (cafeteria and bookstore).

(f) Making purchases from widget machine revenues (camera film, miscellaneous supplies, vehicle car washes, and vehicle tire chains).

(6) Reconciling widget ticket sales to widget machine revenue.

(7) Transporting widget machine revenue to the cashier's office (unlocked bank bags).

(8) Making deposits with the cashier's office.

(9) Reconciling widget machine revenue to total deposits with the cashier's office.

b. Cashier's Office.

(1) Frequency of deposits from the Widget Sales Office.

(2) Identify all personnel from the Widget Sales Office who made deposits.

(3) Indicate how cash receipts were recorded and processed for deposits made.

(4) Number of people present when transmittal bags were opened.

(5) Total bank deposits of (Entity) revenue (unlocked bank bags).

2. Explain the (Entity's) internal controls over widget machine revenue in your area of responsibility.

NOTE: The same information as presented in paragraph 1 above should be presented here for the employee to discuss.

3. Are you generally aware of the provisions of the Whistleblower Program for state employees (Chapter 42.40 Revised Code of Washington)?

4. Do you believe that the Whistleblower Program has been adequately publicized at the (Entity)?

5. If you ever noticed any questionable activities by employees during the normal course of performing your duties, do you feel that you would be able to report these events to (Entity) management officials?

a. If yes:

(1) To whom would you report any such irregular activity?

(2) Do you feel that (Entity) management officials would be responsive to your concerns?

b. If not:

(1) Why wouldn't you feel comfortable in reporting this irregular activity?

6. Have you reported any questionable activities to (Entity) management officials in the past?

a. If so, what did you report?

b. When?

c. And, to whom?

7. Have you ever noticed any employee activity or behavior that you considered to be unusual that you wish to report to the State Auditor's Office at this time?

a. Identify any such employee.

b. What activity or behavior was unusual?

8. Were you at any time aware that one or more (Entity) employees were involved in a scheme to take widget machine revenue prior to the (Entity's) official announcement of this case in (Date)?

a. What advance knowledge did you have of these facts?

b. Who did you obtain this information from and how?

c. Did you report this situation to (Entity) management officials or to the State Auditor's Office?

(1) If so, when and to whom?

(2) If not, why not?

d. Do you know who committed this theft of widget machine revenue funds?

(1) If so, identify any such employee.

(2) How long have you known about this information?

(3) It's in your best interests to tell us everything you know about the circumstances involved in this case. So, please continue with your explanation or elaborate on the facts of the case as you know them.

9. Since the (Entity's) announcement of this loss of funds case, have you become aware of any employee activity or behavior that you consider to be unusual or different in some way when comparing the employee's present and past activities?

a. If so, identify any such employee.

b. What activity or behavior was unusual?

c. Did you report this situation to (Entity) management officials or to the State Auditor's Office?

(1) If so, when and to whom?

(2) If not, why not?

10. Do you think that the one or more employees associated with this loss of widget machine revenue should be severely punished if they were found to be guilty of this act?

a. In your opinion, what should happen to them if they were found to be guilty?

b. Would you be willing to contribute any money to make up for this loss of widget machine revenue?

c. If so, how much?

PRESENTATION OF BANK DEPOSIT INFORMATION

1. We have issued a subpoena to your bank and reviewed your banking activity for all known bank accounts under your control during the period (Dates). If applicable, please review the referenced list of "cash" deposits that were made in these bank accounts during this period of time. I realize that quite some time has elapsed from the dates of these deposits until now. However, to the best of your knowledge:

a. What was the source of funds for each of the listed "cash" bank deposits?

b. What is your explanation for the number and amount of these bank deposits?

c. Do you consider this level of "cash" bank deposits to be normal for your banking activities?

CONCLUSION

1. If an (Entity) employee admits to this theft of widget machine revenue, give them a blank piece of paper and ask them to make a voluntary hand-written statement to document this confession. Make sure that they begin their document by indicating that they are voluntarily making this statement of their own free will. Also, make sure that they indicate the date and time, as well as sign the document.

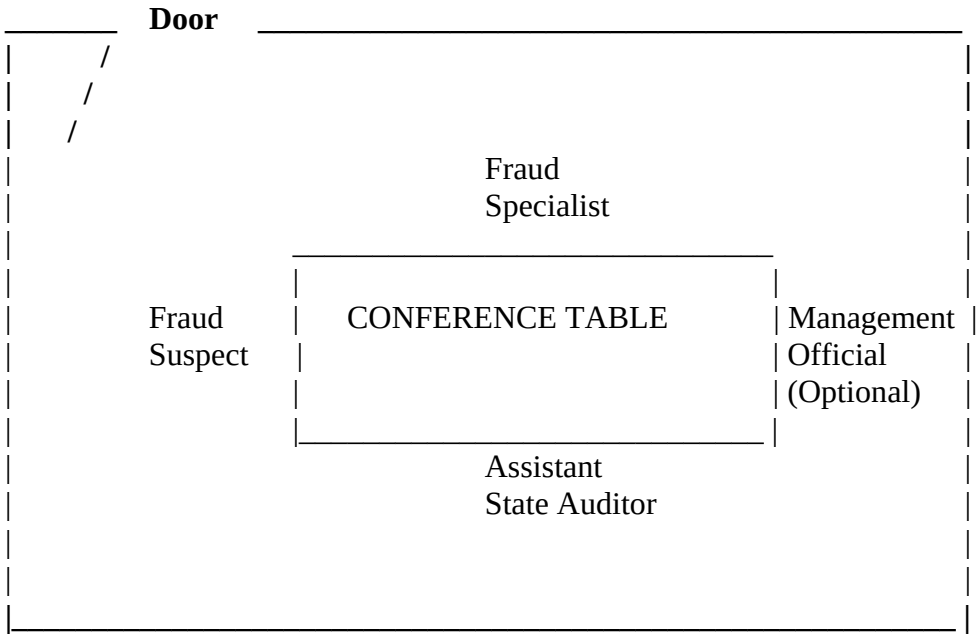
a. If they do not want to make a written statement, do not attempt to coerce them to do so at this time.

b. Refer the individual to (Entity) management officials (i.e.; personnel, legal, supervisor, etc.) for any further disciplinary or personnel action.

2. Request that each person refrain from discussing the contents of this interview with other (Entity) employees to preclude any compromise of this investigation.

3. Thank each employee for their time and assistance during this interview and investigation. Tell them they may leave the interview room and report back to their normal work station.

CONFERENCE ROOM



JRD/SL/JE/18 MAR 97

SUBJECT: Interview with Emma Jane Martin (Jane), accounting clerk at Highline Water District.

SOURCE: District cash receipt records, and assistant state auditors Joe Dervaes, Shawn Lewis, and Jeannine Erickson.

PURPOSE: To document the interview of Jane Martin (Jane) concerning the cash receipting irregularities noted at Highline Water District.

Persons in Attendance.

Joe Dervaes, Jeannine Erickson, and Shawn Lewis representing SAO; Peggy Bosley, General Manager, and Rick Osborn, Finance Manager (acting as Human Resources), representing Highline Water District; and, Jane Martin, accounting clerk.

Details of the Interview.

The interview was conducted in a conference room at Highline Water District. Jane arrived at work at 5:50 a.m. on March 18, 1997, and was immediately brought into the Highline Water District Conference Room by Peggy Bosley and Rick Osborn. Jane entered the conference room and sat in a chair directly next to the door and with her back to the door. She looked directly across the table at Joe Dervaes who conducted the interview. There was nothing blocking her access to the door behind her at any time during the interview. And, she was not compelled to participate in this interview by management or audit officials. The meeting was conducted during normal working hours for this employee using the district's accounting records. The time of the meeting did not interfere with her normal lunch hour, break, or quitting time.

The planning and execution of this interview included making sure that we did not create a "custodial" situation. Assistant State Auditor's of the Washington State Auditor's Office do not have the power of arrest and do not interview government employees in a custody environment. This interview was conducted as an extension of the normal work environment (i.e.; during normal working hours of the employee and using entity accounting records as a basis for the discussion). Therefore, Miranda Warnings do not apply. In addition, since there are no union employees at Highline Water District, Weingarten Warnings do not apply.

During this informal interview, we were merely trying to obtain an explanation for the cash receipting irregularities noted during our audit testing of a $5,912.89 bank deposit on March 17, 1997. If necessary, other cash receipting irregularities noted during our previous audit testing of transactions in September and December 1995 would be presented. However, as the events unfolded during the interview, these prior audit records were not needed during this interview.

Joe began by explaining to Jane that we were here today to talk about the audit work that we had performed on March 17, 1997. Joe first indicated that he and Jane had processed 9 batches of

transactions for deposit on that date. He showed her the documents for these transactions (all of which are further described in his workpaper on the events of the day on March 17, 1997, and are not further detailed here). In all cases, the credits to the customer accounts matched exactly to the checks which were included in the bank deposits. Joe stated that this was the proper method of processing cash receipts at the district, and that this matched management's expectation for this process. Jane appeared to agree with these statements by nodding is an agreeing manner (i.e., shaking her head up and down). However, instead of discussing these batches of transactions any further at this time, Joe stated that he was going to focus on the batch of transactions that was included in the March 17, 1997, $5,912.89 bank deposit which Jane had completely prepared prior to his arriving at the district for the unannounced cash count.

Joe told Jane that this March 17, 1997, deposit was the one for $5,912.89 that Jane had previously acknowledged was "messed up" because the checks in the deposit did not match the account postings to the accounting records for this batch. Jane had previously indicated that there was a normal operating reason for this condition (i.e.; multiple checks for one stub transaction, one check for multiple stub transactions, etc.). However, this condition matched our understanding of prior cash receipting irregularities that we had noted during our prior review of September and December 1995 transactions. Joe then explained that we had completed a detailed analysis of this deposit and that, unlike the other deposits completed yesterday, the checks included in this deposit did not always match the customer accounts credited. Joe asked if she would explain the differences. Jane said that she did not have an answer for the differences. She "didn't know" why this condition would occur. Joe stated that she alone processed this batch of transactions yesterday and that this response was not sufficient. Joe further stated that she did know why this occurred, and we needed to focus on that reason now.

Joe then said that yesterday he had asked her to list and deposit all the checks in her possession. He explained that we had found a batch of checks in her work area between a box of stubs and the trash can near her two-drawer file cabinet, and that these checks had not been included in the batches that were processed yesterday. Joe asked Jane if she had ever seen these checks before. She said that she "didn't know". But, after examining them, she stated that they didn't have her endorsement stamp (i.e.; restrictive endorsement/"For Deposit Only") on them. Joe then addressed the fact that we found the matching stubs for these checks in one of the desk drawers in her work area. Joe asked Jane if she had ever seen these stubs before. Jane didn't audibly answer this question, but rather just shrugged, indicating a "don't know" position in the matter.

Joe then referred back to the March 17, 1997, $5,912.89 bank deposit that Jane said was "messed up". He said that we knew that she manipulated this deposit because some of the checks included in the deposit were related to the batch of stubs that we had just reviewed. Joe indicated that we understood exactly what had happened in this deposit manipulation, but that we wanted to hear it from her. Jane said "What if I said I did?". Joe said we already knew she manipulated the records. Joe then reviewed the lapping scheme that we know exists and further related it directly to the "messed up" deposit.

Joe told Jane that she was probably borrowing money from the district in this lapping scheme. Jane acknowledge this condition by stating "It could be." Joe then picked up a plastic bag containing all the stubs we had found on the floor behind her two-drawer file cabinet and in one of her desk drawers and placed it on the table in front of Jane. He then asked Jane if these were the stubs involving transactions that she had not yet had an opportunity to process. Jane said

"Those are the stubs that I still need to take care of." Joe then asked Jane if all these stubs still need to be entered in the accounting system. She looked in the bag and nodded her head up and down (meaning "Yes").

Joe then asked Jane how much money she had taken doing this cash receipting manipulation. Jane said she "Didn't know". Joe said, "It's gotten out of control, hasn't it". Jane said, "Yes, it's out of control. What do we do now?" Jane seemed to be a little relieved at this point in the interview after admitting to operating the lapping scheme over a long period of time.

Joe said that at this point in our investigation we need to establish the amount of the loss. Joe again asked how much she had taken. Jane said that she "Didn't know". Joe then asked Jane how long this had been going on at the district. Jane said "Not long". Joe said that we know it has been going on at least since September 1995 because the same types of irregularities were noted during our cash receipts testing during the recently completed audit. Jane said nothing. Joe further stated that she had deposits of over $28,000 over the past two years in a U.S. Bank account which was in her name only. He asked her if her husband knew about this bank account. She said "No". Joe asked Jane if this is the account where she put the funds that she had taken from the district. She said "Yes, everything that I have taken is included in that account". At this time, Jane could not remember how long this bank account had been open. As a result, we will have to do additional bank work from the date the account was opened until December 31, 1994 (we already have from January 1, 1995, to the present time on file).

Joe asked Jane if she had manipulated any other transactions at the district besides the daily bank deposits. She said "No". Joe asked her if that was because this was the only area she was able to control. She said "Yes".

The discussion of the irregular March 17, 1997, $5,912.89 bank deposit and Jane's subsequent confession that she had taken money from the district (i.e.; misappropriation of public funds) over an unknown, but rather long period of time, was completed by about 6:00 a.m. Jane was just about finished answering any further questions on the matter at this point. She went silent.

Peggy Bosley then explained to Jane that the district was going to have to terminate her, and gave her a letter confirming this action. Peggy asked that Jane read the letter carefully and then sign it in the designated place. Jane read the letter. The letter states: "As of March 18, 1997, E. Jane Martin is hereby terminated from the employment of Highline Water District for numerous violations of District Policy involving the handling and processing of cash receipts." District due process was further explained in the letter.

Jane then asked how the rest of the district staff would be notified of this situation. When Peggy explained that the staff would be told only that she failed to follow the district's policies and procedures, Jane immediately signed the letter. Then, Peggy Bosley and Rick Osborn also signed the letter on behalf of the district.

Jane stated that she had a lot of friends at the district and hoped that she wouldn't lose them. Peggy Bosley and Rick Osborn indicated that they felt sure the employees would not abandon her. Joe further indicated that management officials and other district employees would not hate her personally. Rather, they would just hate what she did (i.e.; misappropriated public funds). She appeared to feel a little bit better after hearing these words. Jane also wanted to protect her

family, particularly from the publicity that will occur in the future as a result of her actions. However, Joe stated that there was no way to prevent the public from finding out about her actions at the district. When we complete our work, we will issue an audit report on the case. It will be a public document. And, there will undoubtedly be press coverage at that time. This press coverage would occur again when her settlement with the prosecutor is made. She just has to understand that there will be some publicity. It's unavoidable.

Jane said that she would pay back the district for any amount she had taken; but, she wouldn't be able to pay it back all at once. Jane said that the district could take some of these funds back from her by using her entitlements to unused vacation leave, deferred compensation, and retirement. Joe explained that the district could not take those amounts directly from her. Rather, after Jane received these amounts, she could turn over these funds to the district. However, any amounts she paid to the district would not be considered full restitution in this case since the total amount of the loss has not yet been determine by audit. Instead, these amounts would be held in trust as a deposit or partial payment of the full restitution amount (which will be determined as a result of the audit).

Jane then said that she started taking money from the district because of her children and grandchildren (she has a wedding of a grandchild scheduled for this coming weekend). Specifically, one of her daughters needed some financial help. The daughter is a single parent with two teenage children. In addition, she has a severe rheumatoid arthritis condition. This medical condition is so severe that her grandchildren have to help her daughter get out of bed in the morning. It's painful just for her to think about this or to watch the process. Jane stated that she took the money to help out her daughter. She further stated that she did not take the money for her own personal benefit (i.e.; rather, the personal benefit of relatives, specifically her daughter).

Jane then asked about going to jail and prosecution. Joe spoke generally about the process and what sometimes happens regarding perpetrators in white collar crime cases, specifically in cases in state agencies and local governments in the State of Washington (i.e.; except in exceptional sentencing situations -- elements of position of trust, scheme operated over a long period of time, and a large amount of loss in relation to the size of the entity -- sentencing is relatively light). But, this will all be a part of her plea bargain and negotiations with the prosecuting attorney. This part of the case is out of our hands. Our job is to document the amount of the loss and to report (public disclosure). There will be a police investigation. And, the audit and investigation will reach the prosecuting attorney's office for the prosecution phase of the case. Jane stated that she does not want a trial, and will be cooperative in the case. Joe stated that this will undoubtedly help her during the sentencing phase of the case. Joe asked Jane if she had any prior criminal record. She said "No".

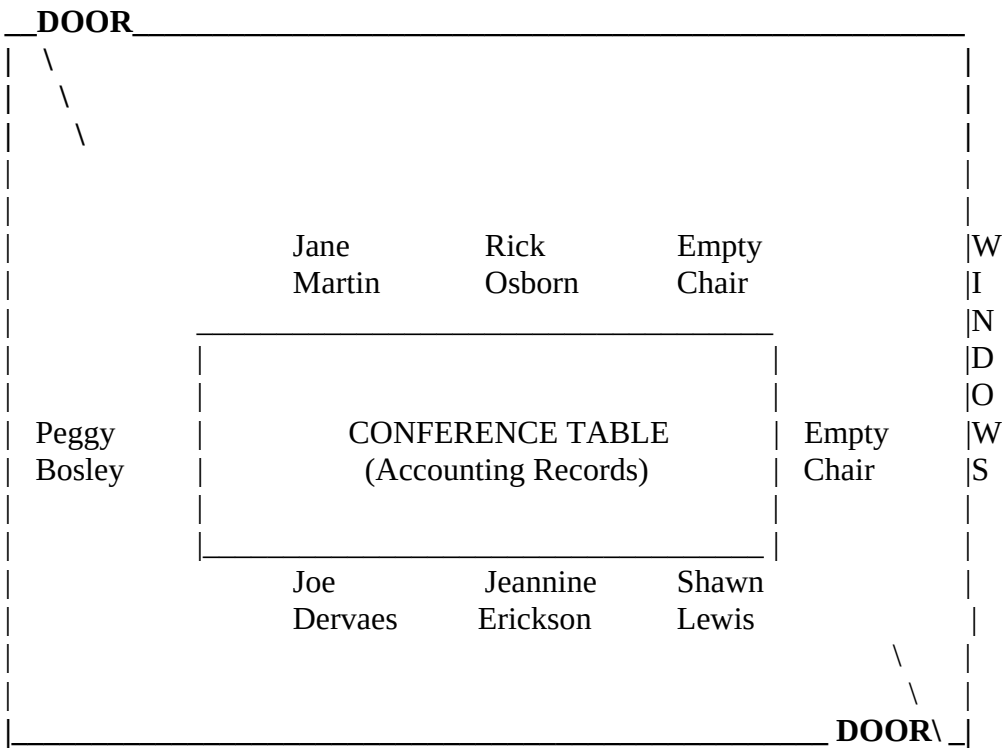
Joe asked Jane if she had any other district records that we might need for our investigation. She said "No", and that all the records we needed were here at the district office. Joe asked her if there was any other area of district operations that we should be concerned about. She said "No". This was all that she did. It was all she had control over at the district. Joe then asked if we could contact her later if we had any further questions about the case. She said "Yes". She then thanked us for making this scheme stop, and said she was relieved that it was finally over. She stated: "Perhaps now I can sleep at night".

The interview with Jane Martin was completed at 6:15 a.m. Rick and Jane left the room to pick up her things from her desk, and relinquish her keys to the office and other items required by the district. Rick had also arranged for another district employee to drive Jane home. Her husband was also at home, although according to Jane, he reportedly knew nothing of this scheme or the bank account where the misappropriated funds had been deposited. So, the most important fact was that there would be someone to be with her during the rest of this day even though she was not very upset over the proceedings of the morning. Based upon the events of the day, Jane was remarkably calm. She did not appear to be depressed and was even quite relieved that her ordeal was over. District managers and state auditors were compassionate during this interview. And, Jane Martin appreciated our position in this case very much.

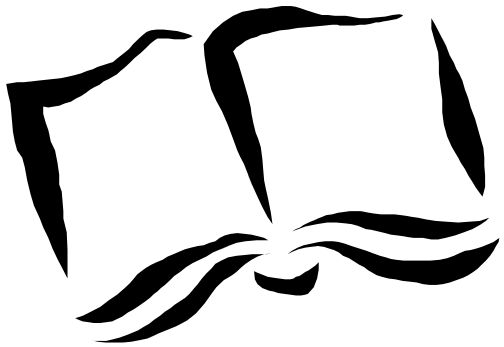
CONCLUSION:

The interview with Jane Martin at Highline Water District has been documented for the audit workpaper file. She confessed to the misappropriation of public funds during the period of her employment at the district. Jane was terminated by the district for numerous violations of policy related to the handling of cash receipts. The amount of the loss has not yet been determined by audit. Jane Martin could not estimate how much the loss was, and could not estimate how long the scheme had operated. She was no help in these areas. This will have to be established by further audit work during this special audit.

HIGHLINE WATER DISTRICT
CONFERENCE ROOM



Fraud Audit Policy



THIS POLICY APPLIES TO:

✓ SPECIAL ENGAGEMENTS
✓ ALL ENTITY TYPES

POLICY 8110 - CONDUCTING FRAUD AUDITS

BACKGROUND

This policy applies to all special audits of actual or suspected fraud, illegal acts, falsification of public records, and conflicts of interest (all categories subsequently referred to as "fraud"), performed pursuant to Chapter 43.09 RCW and other state of Washington rules.

Chapter 43.09 RCW requires state agencies and local governments to immediately notify the SAO of known or suspected loss of public funds or assets or other illegal activity.

Entity managers and SAO auditors must follow correct procedures in order to minimize losses, avoid excessive audit costs, assist in completing audits in a timely manner, expedite the filing of insurance bond claims, ensure proper settlements, and protect employees from false accusations during audits.

REQUIREMENTS

1. Auditors are responsible for notifying their supervisor(s) and audit manager of any suspected fraud immediately upon discovery.

2. Audit managers are responsible for:

- Immediately notifying the fraud coordinator and their assistant director of any suspected fraud.

- Continuously interacting with the fraud coordinator during the life of each fraud audit to ensure SAO managers are made aware of significant events and milestones.

- Sending the following information to the fraud coordinator for each fraud audit:

    a. Insurance bonding policy
    b. Newspaper articles
    c. Judgment and sentencing agreement
    d. Initial notification, status, and closure letters
    e. Other pertinent documents deemed necessary

- Maintaining a log of all important internal and external organizational notifications which occur during each fraud audit.

- Sending a copy of each draft special audit report to the fraud coordinator (in addition to routine distribution to their assistant director) for review prior to conducting exit conferences with entity managers and issuing the report.

3. The fraud coordinator is appointed by the State Auditor to centrally control, monitor, and coordinate all fraud audits. Responsibilities include:

- To the extent possible, promptly conducting on-site visits at all fraud locations.
- Notifying the appropriate county prosecuting attorney and appropriate law enforcement agency of each fraud audit, as well as the cognizant agency if federal funds are involved.
- Advising the audit manager on the timing of internal notifications to entity managers such as the personnel officer or civil service representative, union representative, legal counsel, and agency director or member of the governing body.
- Advising the audit manager and entity managers on the timing of external notifications to law enforcement agencies, insurance bonding companies, the Attorney General's Office, and other agencies as appropriate.
- In most instances, conducting interviews with suspects in fraud audits.
- Reviewing all special audit reports prior to release to the entity, general public, or the media.
- Preparing a monthly status report to keep SAO managers and the Attorney General's Office informed about key events for each active fraud case.
- On behalf of the State Auditor, coordinating with the Attorney General's Office on all written settlement agreements on fraud audits pursuant to Chapter 43.09 RCW.
- Maintaining a data base for the body of knowledge on all fraud audits to assist in preparing and updating materials for internal and external fraud training purposes.
- Preparing an annual report to the legislature on the statistics and results achieved by the fraud audit program.

RELATED POLICIES

Audit Policy 8210 - State Government Whistleblower
Audit Policy 8220 - Local Government Whistleblower
Audit Policy 8230 - Constituent Referrals

REFERENCES

Chapter 43.09 RCW
RCW 43.88.160(6)

THIS POLICY APPLIES TO:

SPECIAL ENGAGEMENTS
ALL ENTITY TYPES

POLICY 8120 - ISSUING SUBPOENAS AND RECORDS SEIZURE

BACKGROUND

SAO has authority to access all financially relevant records and documents (including confidential information) of local governments and state agencies subject to audit, as well as the financially relevant records and documents pertaining to public funding received by private entities. If the entity in possession of the records does not agree to provide them, a subpoena may be needed.

REQUIREMENTS

1. The auditor determines the need for a subpoena.

The auditor makes the initial determination that a subpoena is needed to obtain records and documents to complete an audit. A request is forwarded to the audit manager. If a fraud case is involved, the auditor should coordinate this request for subpoena with the fraud specialist.

2. The audit manager reviews the request for subpoena.

The audit manager reviews the request for a subpoena, and obtains the approval of the assistant director and Deputy State Auditor for Audit Services.

3. The Deputy State Auditor for Audit Services approves subpoenas.

The Deputy State Auditor for Audit Services or his designee will approve or deny any requests for subpoenas and will notify the State Auditor of each approval. The auditor is notified of the approval or denial of the request.

4. The auditor and audit manager prepare the subpoena.

The auditor and audit manager prepare the subpoena using Form A. Initially, the subpoena is sent as an attachment to a letter explaining the authority of the auditor to issue the subpoena and the purpose of the request. See Form B. A provision in the letter requests that the entity not notify the subject individual or public entity of the records request to preclude compromising the investigation. With respect to bank subpoenas, a request is first made for bank statements. A subsequent request is made for specific transactions identified from the initial review.
If the entity refuses to cooperate with the subpoena, the auditor should direct the subpoena to be served by the sheriff in the county where the organization is located. See letter to sheriff Form C.

5. An Assistant Attorney General may assist in the process.

The Assistant Attorney General will assist and advise at any step in the procedure if requested by SAO. If the record holder indicates he/she will not honor the administrative subpoena after service by the sheriff, the Assistant Attorney General should be notified.

The Assistant Attorney General will evaluate the request and may apply to a superior court judge of the proper county to enforce the subpoena.

6. The auditor should not seize records without consent or a subpoena.

If a party holding relevant records needed to complete an audit consents to SAO assuming the possession of records, the original records may be taken into SAO's custody. Such consent must be documented using Form D. In the absence of consent or a subpoena, original records should not be seized.

7. A party may agree to the release of relevant records held by a third party.

If a party agrees to the disclosure of relevant records held by a third party, the financial records release, Form E, should be completed.

RELATED POLICIES

REFERENCES

Chapter 43.09 RCW

FORM A

BEFORE THE OFFICE OF THE STATE AUDITOR
OF THE STATE OF WASHINGTON

SUBPOENA DUCES TECUM

In the name of the State of Washington, GREETINGS:

TO: _____
_____
_____

You are hereby commanded and required to appear at _____, State of Washington at the hour of _____ on the _____ day of _____, 19__ then and thereto testify in the matter of the audit of _____, County of _____, Washington.

You are further commanded to bring with you at said time and place all of the following records, files, and papers pertaining to _____:

_____
_____
_____

for an audit and examination as required by law.

> OPTIONAL: To avoid the necessity of a formal hearing, you may mail the copies of the requested documents to the above address by the specified date.

Please do not notify the individual that this request for personal bank records has been made by this office. Any such action would compromise this special investigation.

This subpoena is issued under the authority of RCW 43.09.165.

Witness my hand this _____ day of _____, 19__.

_____
Title
State Auditor's Office
State of Washington
Phone Number

FORM B

[Date]

[Inside Address]

RE: Subpoena for Personal Bank Records
[NAME]
[Social Security Number]

To Whom It May Concern:

Pursuant to my authority under RCW 43.09.165, I am enclosing a subpoena for personal bank records for any and all bank accounts, whether individually or jointly held with another, at your financial institution in the name of _____ for your information and action. Please research your files for any bank account, whether savings or checking, and notify me of any such account found. If you do not have any record of a bank account, please advise me accordingly.

This information is requested in connection with a special audit of _____, a municipal corporation in _____. Please do not notify the individual that this request for personal bank records has been made by this office. Any such action would compromise this special investigation. I appreciate your cooperation in this most sensitive matter.

This request has two parts.

Part One. Please send a copy of the monthly bank statements for the period of through _____, for any bank account of _____ which is located at your financial institution.

Part Two. After my review of the monthly bank statements from part one of this request, I will make a second request for additional detailed information on specific transactions. I will do this by separate correspondence.

Please mail this information to me at the following address:

[Address]

This letter confirms your agreement to accept delivery of this subpoena (in person) (by US Postal Service) or (by service of an appropriate County Sheriff's Office).

Thank you for your prompt attention to this important matter.

If there is any charge for your research time or the cost of copying this record, please send me a bill for your services when you mail the documents to me.

If you have any questions about this subpoena or request for personal bank records, please call me in _____ at _____. My office hours are from 8:00 a.m. to 5:00 p.m. Monday through Friday.

Sincerely,

[NAME]
[TITLE]

Attachment
Subpoena Duces Tecum

FORM C

[DATE]

Sheriff (or other process server)

Dear _____:

Enclosed are an original and one copy of a subpoena duces tecum for service upon _____ whose name appears thereon.

Upon completion of this service, please promptly return you affidavit of service and your billing on the enclosed voucher.

Alternatively if you prefer to file the original of your affidavit, please promptly furnish us with a copy, along with your billing.

Your early attention to this matter will be appreciated.

Sincerely,

[NAME]
[TITLE]

FORM D

CONSENT TO RELEASE OF ORIGINAL RECORDS

I hereby consent to the release to the State Auditor of the state of Washington and his/her representatives the following original records:

_____

_____

_____

To be used to complete an audit and examination under RCW 43.09._____ (330/state agencies, or 260/municipal corporations).

Dated this _____ day of _____, 19__.

Signature _____

Title _____

FORM E

FINANCIAL RECORDS RELEASE

I hereby authorize and request disclosure to the State Auditor of the state of Washington and his/her representatives, orally or in writing, as may be requested, all information regarding my financial records with _____.

You are also authorized to allow a representative of the State Auditor of the state of Washington to inspect and copy your financial records relating to _____ in your possession.

You may accept a photostat of this authorization with the same authority as the original.

Dated this _____ day of _____, 19__.

Signed _____

DOB _____

SSN _____