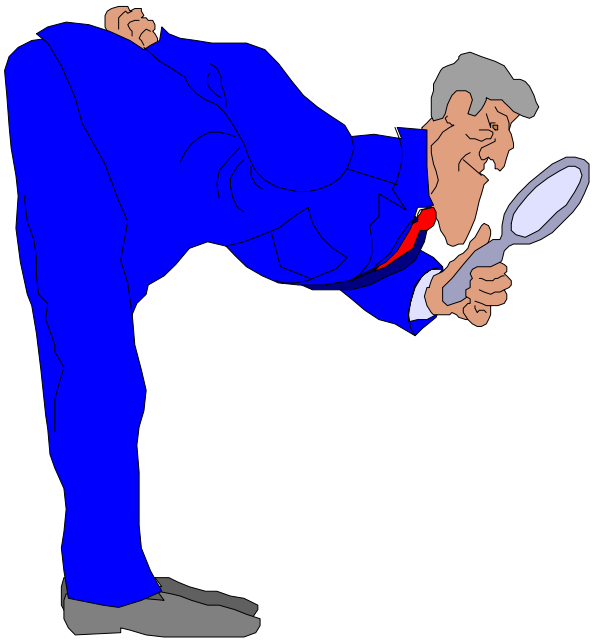


Internal Controls And Fraud

Fraud Manual

Understanding Employee Embezzlement in the Workplace

Author: Joseph R. Dervaes, CFE, ACFE Fellow, CIA
(Retired Auditor and Fraud Examiner with Federal, State, and Local Government Life Experiences)

BIOGRAPHY

JOSEPH R. DERVAES, CFE, ACFE Fellow, CIA
joeandpeggydervaes@centurytel.net – (253) 884-9303

Joe retired after 42.5 years of federal, state, and local government audit service on July 31, 2006. At his retirement, he was the Audit Manager for Special Investigations at the Washington State Auditor's Office where he was responsible for managing the agency's Fraud Program. He specialized in employee embezzlement fraud within all state agencies (170) and local governments (2,400) in the state of Washington. He monitored all fraud audits throughout the state and participated in the investigation of over 730 cases involving losses of over $13 million during his 20-year tenure in this position.

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 U.S. Air Force Lieutenant Colonel. His audit experience includes 20 years with the Air Force Audit Agency and 22.5 years with the Washington State Auditor's Office.

Joe was 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", "Interviewing Techniques", and "The Fraud Interview". He received the agency's "Outstanding Employee Award" five times (1986, 1988, twice in 1999, and 2004).

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. This is the top fraud award in the world and is similar to the Pulitzer Prize in the field of Journalism. Joe is one of the two rank and file members of the Association that have ever been granted this prestigious award. In 2004, the membership elected him to be the Vice-Chair of the ACFE Foundation Board of Directors, one of the highest positions any CFE may hold in the profession. Recognizing his volunteerism and community service contributions, Joe received the ACFE's 2007 award for Outstanding Achievement in Community Service and Outreach. Joe is also a Life Member, Fellow, and Regent Emeritus, and was a previous adjunct faculty member and prior Member of the Board of Review. 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", "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 *Fraud Magazine*, the Association's international journal.

Joe was one of 62 CFEs whose fraud case study was published in a 2007 ACFE book entitled *Fraud Casebook: Lessons from the Bad Side of Business*. Joe was also one of 42 CFEs whose fraud case study was published in a companion 2009 ACFE book entitled *Computer Fraud Casebook: The Bytes that Bite!*

Joe is also the founding and current President of the Pacific Northwest Chapter of the Association of Certified Fraud Examiners (Seattle area) where he is a frequent speaker at Chapter fraud seminars and conferences.

Joe wrote "Fraud Tips" articles for the newsletter of the Association of Public Treasurers (United States and Canada), was a member of the Accounting, Automation, and Internal Controls Committee, and received the organization's Service Award in 1996 and 2005. He is the author of the

Association's manuals on "Techniques for Identifying and Preventing Fraudulent Schemes" and “Stop that Fraud: The Public Treasurers’ Handbook on Fraud Deterrence and Detection”, and also helped develop the organization’s "Internal Controls Checklist".

Joe was active in providing fraud education for the Washington Finance Officers Association. Upon his retirement in 2006 after 42.5 years of government audit service, his public service and fraud educational contributions were recognized by WFOA when it presented him with the award of an Honorary Lifetime Membership in the Association. Joe is one of only a few of the rank and file members of this Association that have ever been granted this prestigious award.

Prior to his retirement, Joe presented fraud awareness seminars to thousands of auditors and management officials from governmental entities and professional associations throughout North America each year.

Class Outline

Page

Part One - Understanding General Fraud Concepts

Planning For Success

General Concepts

The citizens of the state of Washington, and your state or province as well, have two major expectations when they give their hard-earned money to any government. In order to plan for success, the government must:

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

I know that this sounds a bit simplistic. But, it's true. For example: 50 percent of our losses represent cash receipts cases (i.e.; issues with safeguarding the money while under our control), and 50 percent of our losses represent disbursements cases (i.e.; issues with spending the money for authorized purposes).

Just as an aside, fraud is also an equal opportunity activity. For example: 50 percent of our fraud cases were committed by men, and 50 percent of our fraud cases were committed by women. And, there is no typical picture of a fraud perpetrator either. They look just like everyone else you know, and everyone that works in your government. You just never know sometimes. Everyone can do something, and they do what they have access to and can control. That's what segregation of duties is all about. We must do it. Then again, monitoring key functions and activities plays a significant role as well. The reader will certainly hear me say this again.

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",** and it's something they're looking for in order to meet the fraud auditing standards (currently Statement on Auditing Standard No. 99 in the United States). It's part of the professional skepticism that is now required for auditors. But, this is also an extremely important concept for key managers. Always remember that you must **"walk the talk"**, meaning that your actions should match your words. Simply saying that internal controls are important to you and then not implementing the appropriate controls is a good example of what not to do. Employees see your actions and know that you really don't mean what you said in your policies and procedures. In this regard, they know what you do and what you don't do. They are continually watching your actions. If internal controls are not important to managers, they similarly will not be important for the employees of the organization either. It's that simple.

(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. The organization must also **monitor** the work of these employees to deter fraud and to ensure that its expectations are being met.

Managers often tell me that they don't have to worry about fraud happening in their organization because they only hire trusted employees. I wish that were true. But, every fraud perpetrator I've ever met was a trusted employee when they committed the crime. Otherwise, they wouldn't have been able to access the accounting system, manipulate the source documents, and conceal the activity from others. I tell these managers that their common perception is a myth. But, therein lies our dilemma -- to trust, or not to trust? That is the question.

Managers sometimes exhibit "**blind trust**" by telling employees what to do and how to do it, but not monitoring the work of employees to ensure that their expectations are met. These employees are granted the highest levels of access to computers, accounting records, and funds within the organization, and simply ignore or compromise internal controls when fraud occurs. The organization must use the concept of "**trust but verify**". Volunteers from the community or other interested parties could perform this vital work. Periodically reviewing key employee tasks helps to detect irregularities early and ensure that dollar losses are kept to a minimum when, not if, a fraud does occur. Because fraud can never be eliminated, it's essential to monitor activities in a truly periodic and random manner with no discernible pattern of activity. If a manager monitors every Friday, all fraud will take place from Monday through Thursday. Employees who commit fraud study the behavior of managers and auditors, and know exactly how to conceal irregular activity. When they do, they believe they're invisible and bullet-proof.

Another defense to deter trusted employees from committing fraud is a policy requiring all personnel to take vacations each year and be replaced during that time by other employees who actually perform all job functions while they're gone. Another option is to cross-train employees and require them to exchange jobs for specified periods of time.

A Chinese proverb says: "Trust others, but still keep your eyes open." Another wise man once said, "You may be deceived if you trust too much, but you will live in torment if you don't trust enough." For me, this deception comes from blind trust, something managers should avoid at all cost. And no manager should have to live in torment if they practice the concept of trust but verify. There's simply no better way that I know of to help prevent and detect fraud in our midst.

I also believe that the internal controls that should be implemented first are those that protect employees from being unjustly accused when losses occur within the organization. **Two critical issues** associated with this internal control are:

- **Don't tempt employees**. Often employees work alone, primarily at decentralized locations, where they are meeting customers, collecting fees for services rendered, and then taking the appropriate action to ensure the funds collected are deposited into the treasury of the government. If managers do not pay attention to the activity at these locations, employees get the impression that you don't care. It's not true. But, that's where they are, and they have been tempted, often beyond their ability to handle the

situation. It doesn't take long under these circumstances for an employee to decide that your money is now their money. Fraud happens as quickly as that. Now you see it, then you don't. The money is simply gone. The only question remaining is how long this irregular activity will be permitted to exist within the organization before the loss is detected, often quite by accident. Monitoring of these collection activities is extremely important, and you're going to hear that message frequently.

- **Don't put employees at risk**. When multiple cashiers are assigned to one cash or till drawer, funds from all collections are commingled into one container. When, not if, losses occur in this situation, it's impossible for anyone -- managers, police, or auditors -- to determine who was responsible for the loss, even if there are computer cash register passwords in use. The same thing occurs when individuals who store funds in a safe or vault overnight do not have locking containers to secure their funds within the secure facility. When everyone is responsible for money, no one is responsible for money. And, short of a confession from the perpetrator, no one will ever be able to fix responsibility for losses of funds under these circumstances.

(3) Ensure that systems are put in place to monitor all revenue streams. This includes:

- **Identifying all revenue sources and fees**. Many people respond that all funds collected come across their cashier's counter. That's fine. But, you must know what individual revenue streams are processed at each particular location. Be specific. If you don't know what they are today, now is a good time to start making a list. Why? Because many fraud perpetrators misappropriate all, or practically all, of some miscellaneous revenue stream that managers know little or nothing about. That's why they are able to get away with the scheme over long periods of time. Often times these are revenues that simply "drop out of the sky, unannounced one day". In a recent fraud case, managers called these revenues "orphan checks", meaning that they didn't belong to anyone. As a result, they mysteriously disappeared and no one noticed for over five years. The question is, how are you going to handle them if you don't know they exist? Think about it.

- **Determining where the revenues enter the organization**. Again, be specific. If you don't know where the money arrives, you're not in control of the situation. Find out more information about all of the collection points within your organization. There may be more than you know about. And, that would be a problem. Under these circumstances, if the money turned-up missing at one of these locations, who would notice?

- **Including the revenues in the budget**. During this process, managers must decide what analytical procedures are best suited to determine the expected amount of revenue from each source. Don't wait for the auditors to do it. This is a key management responsibility. Auditors know you're in control when you know the answers to questions like this. The budget is an excellent way to monitor all revenue streams. I suggest that they are a lot of revenue streams out there in the world that are not included in the organization's annual budget. Those revenue streams currently represent the highest risk for fraud right now. Identify them for control.

- **Monitoring budget versus actual to ensure that the total amount of revenue matches your expectations.** Someone must perform this task. And, significant variances should be properly investigated by an independent party, someone not associated with the revenue stream right now. Review internal controls over the revenue streams where problems have been encountered. Strengthen them where appropriate. Monitor these activities closely in future accounting periods.

(4) Ensure that systems are put in place to review all disbursements for propriety. This includes:

- All of the important work the staff in the Accounts Payable function performs on a daily basis to ensure that the goods and services described in the documents were actually received at the appropriate location by the proper employee, all payments are being made from original source documents, and all payments are being made for authorized purposes and represent wise business decisions. But, there are many compromises to the internal controls in this important function that challenge financial managers. I'm not going to discuss them at this point in this document. They are covered in great detail at the beginning of the disbursements section of this manual.

- Ensuring 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. There is no better time than now for financial managers to interact and communicate openly with your financial institution. The "bogus" check issue is too great to do otherwise. This is where someone obtains your checking account number and then begins to issue unauthorized checks on your account. You must have procedures in place to address this external fraud risk. We even have cases where the financial institutions have advised local governments to close their bank account because the fraudulent transactions have occurred too frequently. Under these circumstances, you have no choice but to comply. Based upon this scenario, having a large blank check stock on-hand in storage may not be a good long-term business decision these days. Therefore, you should consider an option that allows the printer to periodically deliver checks to you for subsequent use. This would be similar to "just in time" purchasing procedures when the organization orders supplies and equipment.

The degree to which you do all of these things above also 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 – Reporting Requirements

Let's discuss how planning for success applies to managers in fraud cases. The following guidelines apply to state agencies and local governments in the state of Washington and are posted in the Budgeting, Accounting, and Reporting System (BARS) Manual, Volumes One and Two, in Part 3, chapter 12, Interpretation 15**.** It is also posted on the State Auditor's Office web-site (www.sao.wa.gov) at Fraud Program, About the Program**. This information is reprinted here for your reference and future use and is designed to ensure that all fraud cases are properly managed.**

Revised Code of Washington 43.09.185 requires all government to **immediately** notify the State Auditor's Office about all suspected or known losses, including money and other assets, as well as any other illegal activity. It's brief and to the point. Here's what the State Auditor's Office (SAO) says about reporting these matters:

Organizations 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 the State Auditor's Office 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.
- Correct personnel actions are taken.
- Employees are protected from false accusations.
- Bond claims are not jeopardized.

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

- Notify appropriate organization 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 organization 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.

Organizations 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.

Organizations **are not required** to report the following to the State Auditor's Office:

- 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, another state statute, Revised Code of Washington 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 Revised Code of Washington 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.

Planning For Success in Fraud Cases-Facts and Case Development

I have monitored all fraud audits throughout the state of Washington and participated in the investigation of over 640 cases involving losses of over $12.5 million in the past 18 years. My life experiences performing this task have identified a number of critical areas that have occurred in the early life of every fraud case. You need to know about them so that you will be able to successfully handle any fraud case that is detected within your government.

Critical Actions Checklist for New Fraud Cases in State Agencies or Local Governments. This information is designed to ensure that all fraud cases are properly managed. The responsible State Auditor's Office audit team should advise the organization to do at least the following:

- Prepare a chronology document describing the events that led up to the 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

organization 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 organization 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 organization should obtain all office keys from the employee, cancel computer passwords and access, and change any safe/vault combinations if the employee had knowledge or access.

- Protect the applicable accounting records from loss or destruction. This is a very critical step. It's very difficult to investigate or audit a fraud without the appropriate accounting documents. 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 or audit has been completed.

  The organization 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 organization 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 organization 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 organization. After this has occurred, the organization will be able to access the employee's desk without any further concern for privacy issues.

- Inform appropriate organization 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 organization does not have a policy implementing Revised Code of Washington 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 organization is properly handled.

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

  A draft restitution agreement that has been approved for use by the State Auditor's Office and the Attorney General's Office is available upon request from Team Special Investigations. Pursuant to Revised Code of Washington 43.09.260 (local governments) and Revised Code of Washington 43.09.310 (state agencies), a restitution agreement should not be finalized until the State Auditor's Office (Audit Manager for Special Investigations) and the applicable Attorney General's Office 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 the State Auditor's Office audit costs. At the discretion of the organization, it may also include the

organization's internal investigative costs. While the restitution agreement is approved by the State Auditor's Office and the Attorney General's Office, the actual agreement is a unilateral document between the organization and the employee and is signed only by these two parties.

- Ensure that any personnel action is taken based on the employee not following organization 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. There are 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 organization 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 organization 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 organization'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 organization, the victim in the case.

- Notify the appropriate county prosecuting attorney's office having jurisdiction over the organization where the loss occurred. 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 State Auditor's Office may make this notification on behalf of the organization. At the completion of each fraud audit, the State Auditor's Office 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).

Critical Actions Checklist for New Fraud Cases by the Investigator or Auditor. This information is designed to ensure that all fraud cases are properly managed. The responsible investigator or auditor should do at least the following:

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 organization, if anything.

The investigator or 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 organization 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 organization 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 investigator or audit team should also use organization 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 investigator or 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.

Fraud Charts

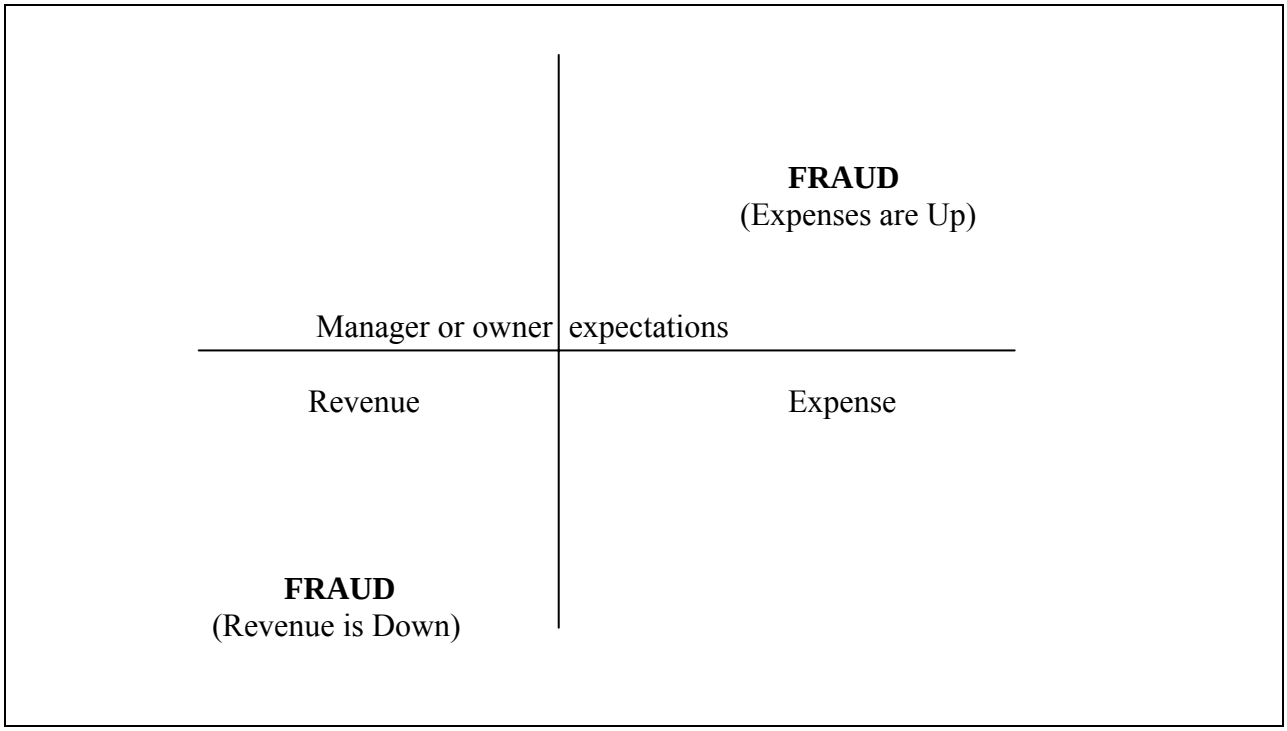
(1) Consider the following chart which depicts manager or owner expectations of revenue and expense when their expectation of business results is a break-even position.

This chart also shows you what the business will look like when fraud occurs in the workplace in such an environment.

 When fraud occurs on the revenue side of the business, the result is that overall revenue is down (from the theft of funds). **The attribute is that revenue is "too low"**. The fraud schemes used may involve unrecorded revenue, such as skimming, or recorded revenue involving other manipulation of the accounting records.

 When fraud occurs on the expense side of the business, the result is that overall expenses are up (from too many expenses representing the theft of funds). **The attribute is that expenses are "too high**". All disbursement fraud schemes used involve recorded transactions. There is also a greater business risk for auditors to detect this type of fraud, because the citizens and stock holders or owners expect fraud to be found in such circumstances.

Thus, auditors must have a different **mind-set** when it comes to designing audit tests to detect cash receipting and disbursement frauds within the organization.



(2) Consider the following chart which depicts a change from good economic times to poor economic times (**such as we are experiencing today in this country**), what happens to internal controls when there is a reduction of employees, and why there is an increase in the risk of fraud within the organization when this happens.

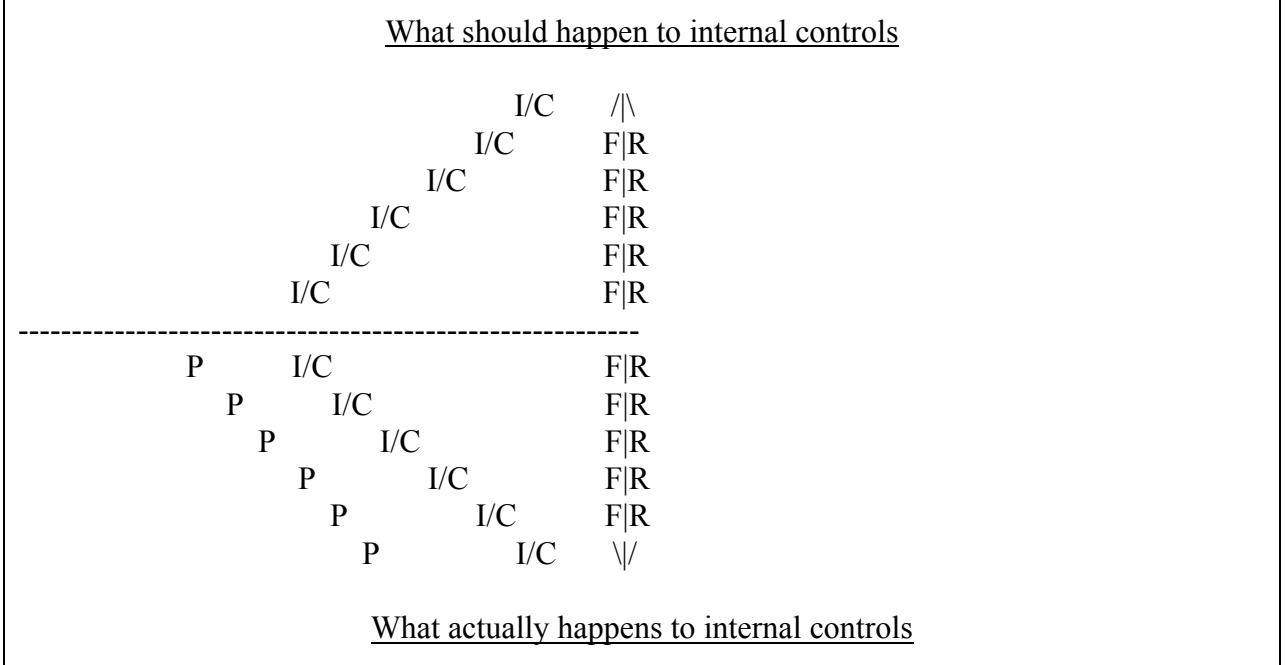
> This chart shows you that in actual practice, internal controls usually **decrease** when there is a reduction in the number of personnel within the organization (as one drops, so does the other – a direct correlation).

However, internal controls should actually **increase** during this period of time (but rarely do) because of the increased risk of fraud on the part of employees who are experiencing the effects of the poor economic times in their individual lives.

This gap in internal controls represents the increased risk of fraud during this period of time.

Please also remember that when there is a return to better economic times, and a return to an increase in internal controls with the organization, some employees retain the duties and responsibilities they obtained earlier which may represent an improper segregation of duties. These employees then use these inappropriate duties to perpetrate (and conceal) frauds within the organization at a later time when, not if they experience tough personal financial situations.

Change in Fraud Risk from Good to Poor Economic Times



Fraud Statistics
Washington State Auditor's Office
January 1, 1987 through July 31, 2006

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**)	484,363
2002	56	1,122,328
2003	62	2,253,394
2004	47	331,803
2005	57	258,960
2006 (**7 Months**)	34	249,528
20 Year Total	732	$13,055,513 (Average = $17,835)
20 Year Average	37	$ 652,776 (Doubled +)

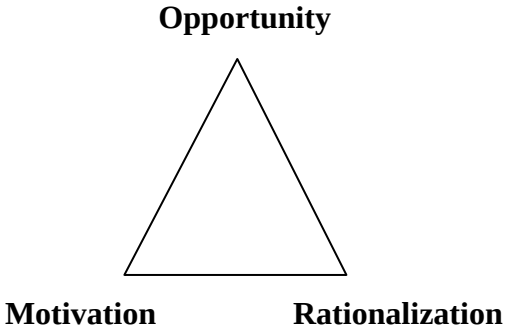
Notes.

(1) The number of fraud cases doubled when RCW 43.09.185 was implemented. This statute required 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 are now being tabulated in the annual fraud statistics.

(2) None of these fraud cases were **material** to the entity's financial statements (in any one year).

The Fraud Triangle
Association of Certified Fraud Examiners

The Association of Certified Fraud Examiners describes the elements of fraud as a **triangle**. The three legs of the triangle are **opportunity, motivation, and rationalization**.



The first leg of the triangle.

Opportunity always comes first. All employees have a certain degree of opportunity within the organization. It's unavoidable. The internal control structure is designed to deal with this condition. But, when appropriate safeguards are not put in place to monitor the work of key individuals, the organization creates a climate that gives the trusted employee the opportunity to do things they might not ordinarily do. Sometimes the organization creates this fatal flaw by tempting employees beyond their ability to handle the situation. This is a tragic mistake.

These employees have all the important ingredients that allow them to commit fraud, including **access, skill, and time**. Again, all employees have these ingredients in varying degrees. But, it's the trusted employee who is granted the highest levels of **access** to the organization's computers, accounting records, and funds. The organization has also trained these employees in order to perform its mission and to operate efficiently. So, the trusted employee has all the requisite **skills** needed to perform their job. But, they often do this in ways the organization never intended. Finally, every employee is given the **time** necessary to accomplish the tasks assigned. When fraud is present within the organization, we often pay these employees overtime to commit the fraud.

The second leg of the triangle.

Motivation is the next critical element. It includes **financial need, challenge, and revenge**. When the trusted employee has a **financial need** in their life, the motivation factor kicks in to permit the individual to perform an illegal act. The financial need can be either real or perceived (i.e.; greed). They become desperate and see no other alternative to solve their financial crisis. Sometimes this is the most visible element of change in a person's life actually observed by fellow employees in the office. But, sometimes the individual commits fraud by exploiting the organization's computers, accounting systems, and internal controls as a **challenge**. Breaking

the organization's codes and passwords is perceived as a game. The most dangerous person is one who seeks **revenge** against the organization. This wayward employee seeks to financially destroy the organization in retaliation for the poor treatment they've received in the past. Employees who have lost their jobs, been passed-over for promotions, or who did not receive a raise fall into this category.

The third leg of the triangle.

Rationalization is the final piece of the puzzle. It's not far behind the other pieces because this trusted employee is definitely at the center of the organization's financial world. They're important, and they know it. **Justification** takes control of them as they proceed on this course of destruction. They've convinced themselves that they're entitled to the organization's assets, and feel no remorse about taking the resources either. After all, they're overworked and underpaid, and you owe them. Besides, they're already interpreted the organization's actions to mean that it doesn't care about the resources being misappropriated anyway (rightly or wrongly, it makes no difference). In their own mind, they're right. They sleep well at night.

The Trusted Employee

So, who is the person that would commit fraud within your organization? Ultimately, the answer is **the trusted employee**. And, this person can work anywhere within the government.

The trusted employee is indispensable to the organization. When this employee commits fraud within the organization, **the chameleon effect** begins. This person changes from an honest person to a dishonest person overnight. Sometimes very subtle changes occur in the way this individual performs their job. They're just not the same person anymore. But, because of their key position in the organization, no one seems to notice. Like the chameleon, they blend in with their surroundings to avoid detection and become perhaps the organization's worst nightmare -- **the trusted employee gone wrong**.

When the trusted employee begins to misappropriate the organization's resources, they're also in a position to manipulate the accounting records and to keep the fraud from being detected, often for long periods of time. Most employees who misappropriate funds from their employer **act alone**. These individuals are convinced that they're **invisible and bullet-proof**. They believe that others around them cannot see what they're doing. Besides, they're very clever.

The trusted employee initially does not come to work planning to steal from their employer. This is always true for honest people in the world. But, this is never true when the organization hires a **dishonest employee**. This person immediately begins their quest for a position of power, one that controls money. If they weren't hired for such a position initially, they begin to work their way through the organization by transfers and promotions until they find the position that suits their purposes. The best defense against this person is simply don't hire them. Thus, the organization should do everything possible to perform background investigations that at least uncover terminations and criminal convictions for misappropriating funds from their prior employer(s).

But, what about the **honest employee**? Does the organization have to worry about them too? Of course, the answer is "Yes", but not nearly as much as the dishonest employee. The real problem is that the organization often puts this thought completely out of their mind over time. The organization is lulled to sleep by repetitive good behavior. These employees don't usually start to misappropriate public funds right away. But after awhile, they've been around long enough to see weaknesses in the internal control structure in their area of responsibility. They might even have been tempted beyond their ability to handle the situation. As a result, they often make unwise decisions and begin to take advantage of the situation, and the organization, to profit personally. This is when the fraud begins.

So, what should an organization look for to determine whether a **trusted employee** might be misappropriating funds from the organization? As indicated below in "the system of internal control" document, supervisors are a greater risk than "doers". However both categories of employees can and do commit fraud. The reason for this is that most internal controls are designed to ensure that supervisors review the work of others, the "doers". That leaves the organization vulnerable in the supervisor category since few organizations review the work of this truly trusted employee in the same way they review the work of their subordinates. In fact, organizations sometimes trust these employees to a fault (i.e.; **blind trust**).

The answer to this question starts with the primary internal control weakness present when fraud occurs. Of course, **the culprit is segregation of duties**, as described in the following section.

But first, I want you to consider some additional information about the trusted employee. The following information came from an article I wrote recently for the newsletter of an association of cities in the state of Washington. Some material from this presentation will be repeated in the article. But, I feel this repetition will reinforce this important message about fraud. The article was entitled "**Trust, But Verify**".

Today, more than ever before, Mayors and Council Members of small cities and towns are being called upon to take a more active role in meeting the citizen's expectations of safeguarding funds from loss and spending money for authorized purposes. Because of limited staffing, these key managers may be the only line of defense against fraud. But, many may not see this as their role. This can lead to tragic consequences.

Managers often tell me that they don't have to worry about fraud happening in their organization because they only hire trusted employees. I wish that were true. But, every fraud perpetrator I've ever met was a trusted employee when they committed the crime. Otherwise, they wouldn't have been able to access the accounting system, manipulate the source documents, and conceal the activity from others. I tell these managers that their common perception is a myth. But, therein lies our dilemma -- to trust, or not to trust? That is the question.

Managers sometimes exhibit blind trust by telling employees what to do and how to do it, but not monitoring the work of employees to ensure that their expectations are met. These employees are granted the highest levels of access to computers, accounting records, and funds within the organization, and simply ignore or compromise internal controls when fraud occurs. Therefore, periodically reviewing key employee tasks helps to detect irregularities early and ensure that dollar losses are kept to a minimum when, not if, a fraud does occur. Because fraud can never be

eliminated, it's essential to monitor activities in a truly periodic and random manner with no discernible pattern of activity. If a manager monitors every Friday, all fraud will take place from Monday through Thursday. Employees who commit fraud study the behavior of managers and auditors, and know exactly how to conceal irregular activity. When they do, they believe they're invisible and bullet-proof.

What are some of the common problems commonly seen? Employees have incompatible duties such as:

- Acting as a bank account custodian but also performing the monthly bank reconciliation.
- Acting as a cashier but also preparing the daily bank deposit.
- Preparing input in accounts payable or payroll but also having access to the output (the checks).
- Preparing customer accounts receivable billings, cancellations and adjustments (write-offs) or entering accountable documents into the computer database, but also acting as a relief cashier.
- Acting as a cashier, but also reconciling the bank deposit information with the organization's accounting records related to the accountability for funds.

What are some of the common fraud issues encountered in small cities and towns as a result of segregation of duties problems? Employees:

- Take funds from every revenue stream, including utilities, animal control fees, court fines and fees, marinas, etc.
- Take money from change funds and imprest fund accounts, or from daily bank deposits.
- Purchase items for their own personal use using gasoline and procurement credit cards or the petty cash fund.
- Manipulate their own payroll records for salary, leave, and other benefits.

To solve segregation of duties problems and to reduce claims for losses from the insurance pool (something that we use in the state of Washington instead of purchasing insurance from a commercial carrier), hire two employees to perform the duties or split the duties among two or more employees. If the organization can't do either of these procedures it should establish a monitoring program for this key employee. And, this is where the Mayor or Council Member may be the primary source of help. Or, volunteers from the community could perform this vital work.

Another defense to deter trusted employees from committing fraud is a policy requiring all personnel to take vacations each year and be replaced during that time by other employees who

actually perform all job functions while they're gone. Another option is to cross-train employees and require them to exchange jobs for specified periods of time.

A Chinese proverb says: "Trust others, but still keep your eyes open." Another wise man once said, "You may be deceived if you trust too much, but you will live in torment if you don't trust enough." For me, this deception comes from blind trust, something managers should avoid at all cost. And no manager should have to live in torment if they practice the concept of trust but verify. There's simply no better way that I know of to help prevent and detect fraud in our midst.

Segregation of Duties

Remember, everyone can do something, and people do what they have access to and can control. This is what allows them to conceal irregular or fraudulent activity in the first place. Therefore, a person with a **segregation of duties** problem is the one person within the organization that is the greatest fraud risk.

Problem: Employees who:

- Control a transaction, process, or function from beginning to end. This is **not** usually the entire system of cash receipts or disbursements, but rather a small slice of the world, one that many managers would perhaps not even notice. This includes such things as an employee who:

- Primarily serves a bank account custodian, but also performs the monthly bank reconciliation.

- Primarily acts as a cashier, but also prepares the daily bank deposit.

- Primarily prepares input in accounts payable or payroll, but also has access to the output (the checks) – what I call the "kiss of death" in disbursement frauds.

- Have other incompatible duties. This includes such things as an employee who:

- Primarily prepares customer accounts receivable billings, cancellations and adjustments (write-offs), but also acts as a relief cashier.

- Primarily enters accountable documents into the computer data base, but also acts as a relief cashier.

- Primarily acts as a cashier, but also reconciles the bank deposit information with the organization's accounting records.

Solution: First, hire two employees to perform the assigned duties when a segregation of duties problem exists. If this is not possible, split these duties between two or more existing employees. Finally, if the organization is not able to do either of the above, it must establish a monitoring program for this key employee that effectively accomplishes a segregation of duties without hiring or using two employees to do the job, such as by having an independent party monitor key employee tasks.

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 any misappropriation 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 organization 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.

Brief Checklist to Identify "At Risk" Employees

An employee with unusual work habits, such as an individual who (**do you see yourself?**):

- 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.

The Issue Is Control!

Examples from actual fraud case studies:

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.

The System of Internal Control

Key internal control structure responsibilities are as follows:

Management: Establish and monitor internal controls.

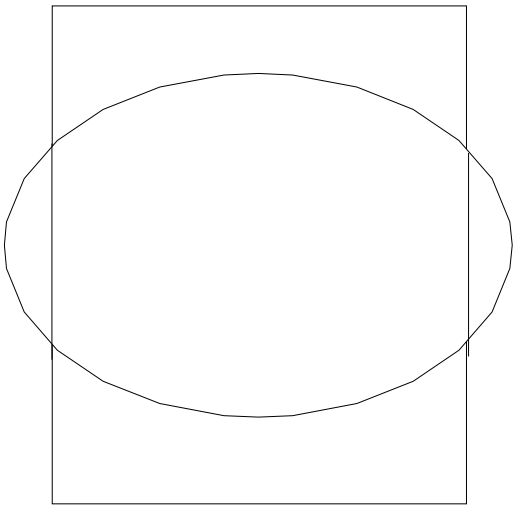
Audit: Evaluate and test internal controls.

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

- Ψ Ignore internal controls established by management.
- Ψ 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:

- If you have not already obtained a bank-validated deposit slip indicating the actual check and cash composition of the bank deposit, contact your bank to obtain a sample of these documents from the bank's microfilm records.

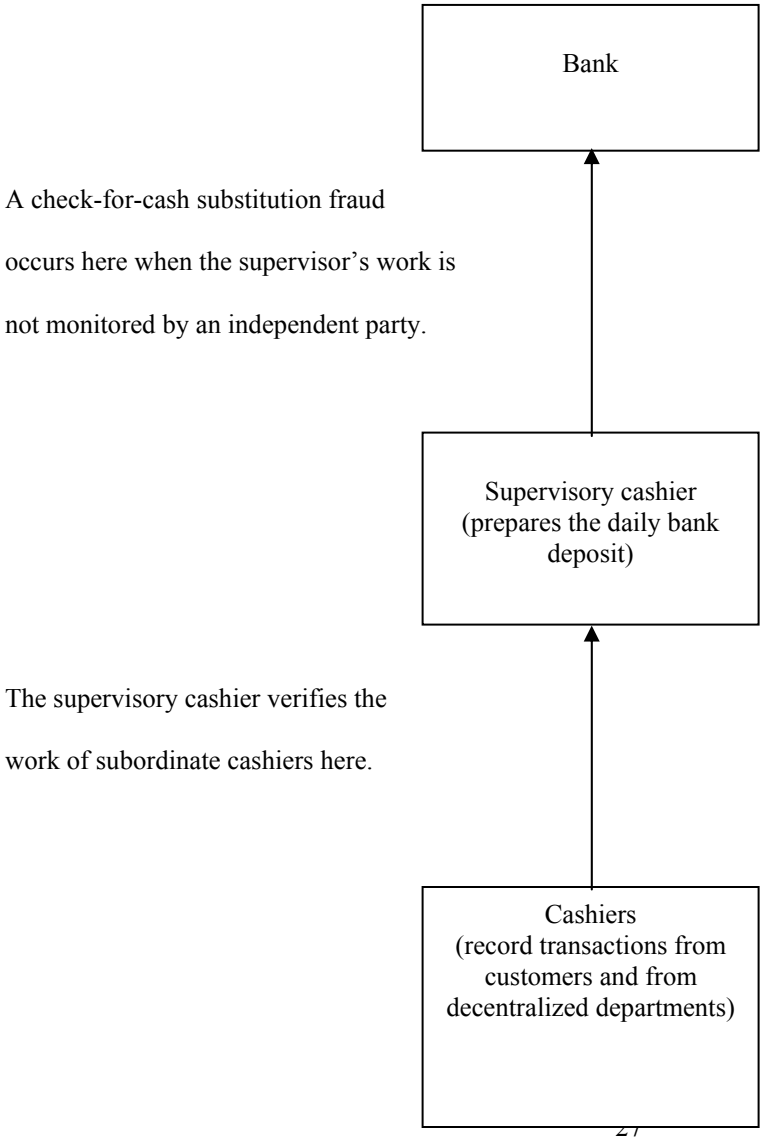
- If you have on-line banking capabilities for the depository bank account, verify the check and cash composition of the actual bank deposit from the bank's records. Copy the bank deposit slip to provide evidence of this monitoring action.

- 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.

Cash Receipting Example

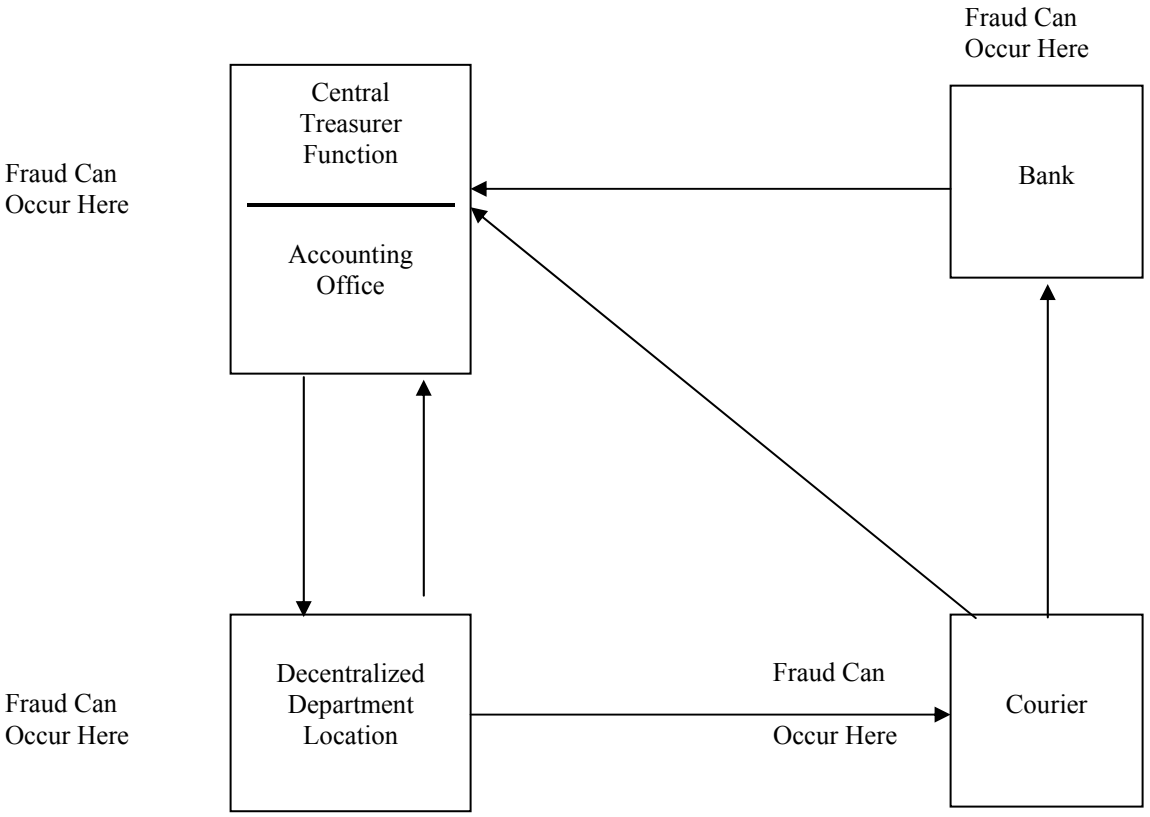


(2) Lack of fixed responsibility for funds (and losses) is the second problem.

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 Washington with no fixed responsibility for the loss is way too high, and demonstrates that too many managers incorrectly deal with this risk today.

Solution: 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 inside the safe or vault. **Employees must sign receipts for accountability purposes when funds are transferred from one person to another.** 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?"

Decentralized Location Cash Receipting Flow Chart Example



Decentralized Location Cash Receipting Flow Chart Example – Description of Procedures

Decentralized department location collect funds from customers for services rendered and record transactions on manual cash receipts, cash registers, or computer cash registers by mode of payment.

Decentralized department location counts funds and balances to recorded receipts by mode of payment and prepares a daily activity report.

Decentralized department location sends a copy of the daily activity report to the central treasury function/accounting office.

Courier picks up bank deposits daily from the decentralized department location, sometimes signing a transmittal log to acknowledge receipt of the funds, and sometimes not. What about fixed responsibility?

Courier prepares a consolidated daily bank deposit for all decentralized reporting locations indicating the check and cash composition of funds on the bank deposit slip.

Courier sends a copy of the consolidated bank deposit slip indicating check and cash composition of funds to the central treasurer function/accounting office. If the consolidated bank deposit slip is falsified (cash shortages), discrepancies may be noted on a daily or monthly basis, depending upon the procedures used by the central treasurer function/accounting office to reconcile decentralized department location daily activity reports with information from the bank deposits the courier actually made. (**CRITICAL**)

Bank sends a monthly bank statement to the central treasurer function/accounting office.

Central treasurer function/accounting office reconciles bank deposits made per the duplicate copy of the consolidated bank deposit slips received from the courier and from the monthly bank statement received from the bank with the daily activity reports received from the decentralized department locations, sometimes on a daily basis (preferably), and sometimes on a monthly basis (possibility of a delay in reporting any irregularities). Discrepancies are investigated and reported.

Central treasurer function/accounting office codes all revenue transactions for daily input into entity's computer accounting system.

Central treasurer function/accounting office sends a monthly financial report to all decentralized department locations.

Decentralized department locations reconcile total revenue collected with the amounts shown on the monthly financial report. Discrepancies are investigated and reported. (**CRITICAL**)

Case Study: Edmonds School District - $143,150

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 and using a lapping scheme to conceal the irregular activities, 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 the complex manipulations in the District's daily bank deposits during this period of time, it was not practical or cost effective to determine the full extent of this loss. The loss was covered by the District's insurance bonding policy. The employee was sentenced to 13 months in the state penitentiary.

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 (Red Flags). 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.

Sentencing: The employee was sentenced to 13 months in the state penitentiary.

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 organization 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.

Fraud/High Risk Decision Process
(Auditor or Manager Mindset)

(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).

Index to Fraud Schemes in SAO Fraud Training Manual

Cash Receipting Fraud Schemes

Disbursement, Accounts Payable, and Payroll Fraud Schemes

Purchasing and Contracting Fraud Schemes

Part Two – Understanding Cash Receipting Fraud Schemes

Skimming

Skimming currency from customer payments is quite simple. That's why it's the crime of choice and the most common form of cash receipts fraud. **The actual amount of losses from skimming is unknown, and most schemes are not detected. The primary suspect is a cashier**. The cashier merely has to talk customers out of a receipt or give them a bogus cash receipt form for any transaction for services rendered by the organization. Either method works if the customer isn't concerned by either of these conditions and if the organization hasn't implemented internal controls over the revenue sources at this location. Business continues normally, and everything appears to be just fine. But it isn't.

To detect this type of fraud, listen to what cashiers say when they interact with customers. The highest risk question from any cashier is: "Do you need a receipt?" If the customer says "yes," the cashier receipts the transaction and is then accountable for the funds. If the customer says "no," or if the casher gives the customer a bogus cash receipt form, the funds received from these transactions basically represent "free" money, because there was no accountability established for the revenue from this transaction. Using video cameras in the cashier area helps to deter skimming by cashiers. Using some alternative method of determining sales (such as the number of units sold times unit price equals revenue) also works, but with limited success in retail businesses where there are too many variables in unit prices. Getting sales recorded is the issue.

Cashiers operating cash registers anywhere, such as at restaurants, bars, coffee houses, and retail sales establishments, often operate with an open cash drawer. When customers make payments for purchases, cashiers merely make change. The amount of money received from these sales is simply stolen. This is skimming of currency from customer payments at its best. And it's happening every day of the year in businesses all over the world. It's the primary reason business try to separate cash receipting from product delivery, such as in fast food restaurants.

The same thing also happens when a customer makes a payment with a check. Sometimes a cashier will tell a customer to leave the payee area on the check blank because he or she has a rubber stamp with the organization's name. A crooked cashier will write his or her name or the word "cash" on the payee line of the checks and either cash them at a financial institution, or deposit them into his personal bank account. Sometimes the cashier will tell customers that their canceled checks are their receipts or that receipts aren't issued at the facility. When these check transactions aren't receipted, a crooked cashier often substitutes them for cash that has been received and recorded from other transactions on the same business day (i.e.; a check for cash substitution scheme). The cashier easily removes an equal amount of currency from the cash register till drawer at any subsequent time during the day and keeps the money for personal use.

These losses hit the organization's bottom line immediately. Indications of these irregular activities later appear in inventory shortages that are written-off as expenses and then decrease the organization's net income. Rarely do these fraudulent activities force an organization into bankruptcy or put them out of business. But the reduced amount of revenue from operations

certainly does hurt the organization's overall financial picture. Also, the government doesn't receive sales tax from these unrecorded transactions. Consumers actually pay a theft tax for skimming losses, shoplifting by customers, and the theft of merchandise by employees in the form of higher retail prices.

Skimming currency from customer payments for services rendered by the organization most often occurs at a decentralized location where there is only one employee on duty. In such circumstances, there is no one present to observe how transactions are handled or to independently determine if all transactions have been processed as required. But, cashiers at central treasury facilities use the same methods that employees use to skim revenue at decentralized locations. However, because of the number of employees involved at these facilities, managers normally implement internal controls over cash receipts by segregating duties among employees and instituting improved cash receipting systems for all funds received. These funds include payments from customers and all money transmitted to the central treasury facility by decentralized locations. However, even these procedures don't deter an unscrupulous cashier from skimming currency.

A customer rarely "sees" the fraud involving their transaction because the process is so relaxed and comfortable. The customer wants the transaction completed quickly with minimal disruption of their life so he or she can resume their daily routine. A crooked cashier knows this and simply smiles while telling the unsuspecting customer to have a nice day. As soon as the customer departs the facility, the cashier steals the funds.

The revenue sources employees choose for skimming include all types of miscellaneous revenue that aren't controlled by accounts receivable systems. Even though managers know this scenario provides an incentive for unscrupulous employees to steal funds, they often don't implement internal controls to protect the revenue sources generated throughout the organization. From time to time, even some honest employees are tempted and cross over the line from being honest to becoming dishonest.

Case Study: King County Solid Waste Division - $162,500

Four cashiers and machine operators skimmed at least $162,500 in revenue from the Hobart Landfill site during a one-year period. The investigation by the internal auditor included the use of covert surveillance techniques (i.e.; videotape cameras) to record the cash receipting activities of landfill employees and analytical procedures on the historical cash receipting activity of individual landfill cashiers. The loss was covered by the county's insurance bonding policy. Three employees were sentenced to three months in the county jail. The fourth employee was sentenced to two months in the county jail.

Money Laundering Activities
(Methods Employees Use to Convert Organization Revenue and Disbursement Checks for Personal Benefit)

An inappropriate segregation of duties is at the heart of every fraud case. That's what allows the fraud to occur in the first place and then go unnoticed for what is often a long period of time. **These frauds occurred because cashiers received revenue checks from customers in the normal course of business but did not record the transactions in the organization's accounting system.** As a result, there is no accountability for the funds. It's "free" money to the employees.

If these were checks that employees cashed out of the cash receipts of the business day, we would not be quite as concerned. This is an internal control weakness in operations. But, it's not fraud.

In this fraud scheme, we're talking about your hard-earned revenue checks that represent legitimate payments made by customers for a service provided by the organization. These funds should be in your treasury.

What the employees choose to do with these unrecorded revenue checks is depicted below. In this discussion, "money laundering" is the process the employees use to negotiate the checks in order to obtain the proceeds for their own personal benefit.

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**. Did you hear that? We must listen! 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 in the state of Washington were $890,070 (18.6% of all dollar losses).

Solutions: 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.

Check for Cash Substitution Scheme

A check for cash substitution scheme is the primary 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. **In the state of Washington, this scheme accounts for 10% of all fraud cases, but 25% of the dollar losses ($4 million over 20 years). This is the crime of choice for a supervisory cashier, one who makes the bank deposit without anyone ever looking at its composition. The prime suspect is the person who makes the bank deposit.** You have to pay attention to this scheme.

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".

Case Study:
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 a list/log of all checks received, and then compare the amount of 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 organization 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 organization. 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 organization'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 organization 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 organization 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.

Lapping Scheme Training Example

The following is an example of a lapping scheme fraud which uses three customers who each owe $100 in an organization's accounts receivable system:

Customer "A" pays $100. An employee misappropriates these funds. The $100 loss of funds remains with this customer.

Customer "B" pays $100. This payment is credited to the account of Customer "A" who is made whole by this transaction. Now, the $100 loss of funds remains with this customer.

Customer "C" pays $100. This payment is credited to the account of Customer "B" who is made whole by this transaction. Now, the $100 loss of funds remains with this customer.

The loss begins with Customer "A", but ends up with Customer "C".

The "**net cumulative effect**" of these account manipulations is that an employee has misappropriated a $100 payment from Customer "C". It is the sole remaining account that has not been credited with the proper payment. A list of these accounts must be prepared to provide the amount of loss in the case. Attempting to find all of the manipulated accounts in the scheme is fruitless.

Fraud perpetrators must maintain accurate records in order to conceal the irregular activity. Mistakes ultimately bring down these schemes. It just takes one valid customer complaint to bring down the scheme. Disaster then strikes with devastating results.

An important issue is that an independent party must resolve all customer feedback (complaints). This is essential for fraud detection purposes.

Ways perpetrators conceal the disposition of lapping scheme losses

There are a number of ways fraud perpetrators attempt to conceal the disposition of lapping schemes. Some of them include:

Making restitution or pay back the amount of the loss, either secretly or by informing the organization.

Canceling the accountability established by the cash receipts issued, such as by unauthorized voiding activity.

Destroying the supporting documents representing the accountability for the funds stolen.

Reporting a mysterious disappearance theft of cash receipts. This is a bold attempt to conceal the losses of any lapping scheme.

Accounts Receivable Fraud Schemes

Accounts Receivable – Internal Control Structure - Duties of Personnel

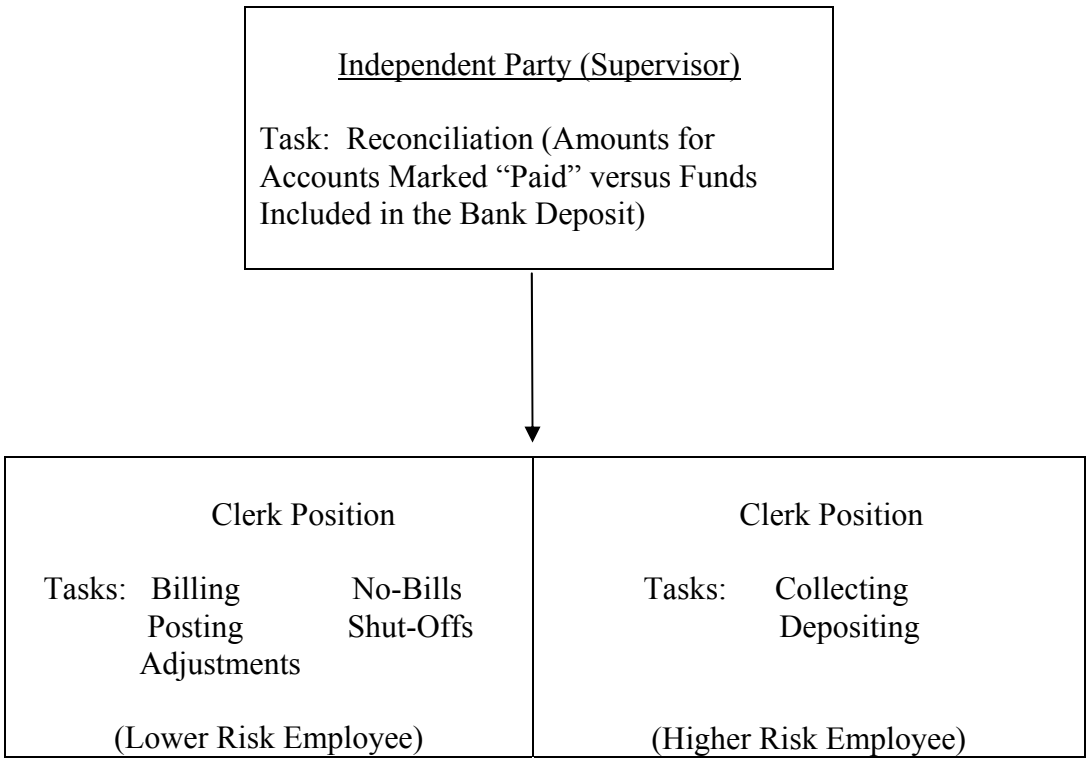
The ideal separation of duties for employees working in the accounts receivable function is as depicted in the diagram shown below. Three employees are needed. But, this is not always possible. Therefore:

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).

Chart Depicting Segregation of Duties in Accounts Receivable Systems



Types of Accounts Receivable 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.

- Eliminating Customer Accounts.

In certain organizations, 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, and 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 are simply 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 organization 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.

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 organization 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.

Determine if there is <u>any</u> (or a sufficient amount of) <u>cash</u> in the daily bank deposits.

Steps to Detect Fraud in Accounts Receivable Systems

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 organization 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 organization 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 organization 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.

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 and monitoring is required for these transactions.

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 organization 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 organization periodically review their records to see if their expectations are being met?

Does the organization know which customers pay their account in cash? These accounts might also be "flagged" in some way for identification purposes within the organization's computer system. The organization 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)**.

Case Study: Highline Water District - $357,237

Scheme. Lapping scheme in a utility accounts receivable system for an undetermined amount of time. 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 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 seven audit steps from the 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.

Case Study: 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 a utility accounts receivable system environment. All cash receipt transactions were first processed on a cash register system which produces data for the city's financial statements. At the end of the business day, these transactions were interfaced with another utility accounts receivable system (stand alone computer) which marked all customer accounts "paid". The utility clerk then reversed the initial transactions from cash register system and re-entered only customer's accounts paid by check (lesser amount). The cash register 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 checks 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 checks, 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 cash register system with the 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 checks 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 checks.

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 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 accounts receivable 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 in a work release program.

Case Study: City of Poulsbo (Municipal Court) - - $290,227

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. The Court's computer 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 Court's computer accounting system.	$ 5,127.00
There were 49 irregular transactions between 03/03/98 and 12/12/02.	
Collection agency payments were never recorded at the Court.	285,100.45
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.	
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 computer 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 (Red Flags). 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 Court's computer 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 Court's computer 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.

Other Cash Receipting Fraud Schemes

There are, of course, many other cash receipting fraud schemes. However, there would never be enough time for us to cover then in any detail. So from my life experience dealing with fraud in the state of Washington, some limited coverage of these fraud schemes is presented below:

Cash register schemes (voids, refunds, paid-outs, and missing "Z" tapes).

Computer cash receipting schemes (non-cash credit transactions, such as community service and jail time in courts).

Placing personal checks in the till drawer (borrowing schemes, where all fraud starts).

Establishing your own accountability (the most dangerous person in any organization).

Altering cash receipt forms after issue (identifying the attribute of ink versus carbon on the accounting copy of receipts issue is the key to detection of these schemes).

Multiple cash receipt books (one for the organization, and one for the cashier - finding them is critical to detection of these schemes).

Making short bank deposits (this is more common than you might think–account for the universe of all revenue transactions).

"Free" access to safes and vaults (no fixed responsibility for funds is the issue).

Not requiring decentralized locations to make direct bank deposits (transmittal systems must be secure).

Retail sales activity (normally present in schools, but applicable to retail sales operations in any organization).

Checking account schemes (cashing entity revenue checks and taking "cash back" from an official bank deposit – money laundering is the issue).

Establishing bogus organization checking accounts (misappropriation of revenue by money laundering is the issue).

Part Three: Understanding Disbursement and Accounts Payable Fraud Schemes

The ultimate objective of any disbursement scheme is a check issued by the organization which is then converted to cash for personal gain. Managers often think that the check issuance process is unimportant. After all, it's just paper.

In state agencies in Washington, this type of fraud accounts for 85% of all losses over the past decade. It's too big to ignore, and very easy to defend against. The prime suspect is the bookkeeper.

The most common disbursement fraud involves a bookkeeper who issues checks to themselves or to others (i.e.; family and false vendors). Looking at the redeemed checks is the primary defense against this fraud. Knowing who you do business with is the primary defense in identifying checks issued to false vendors.

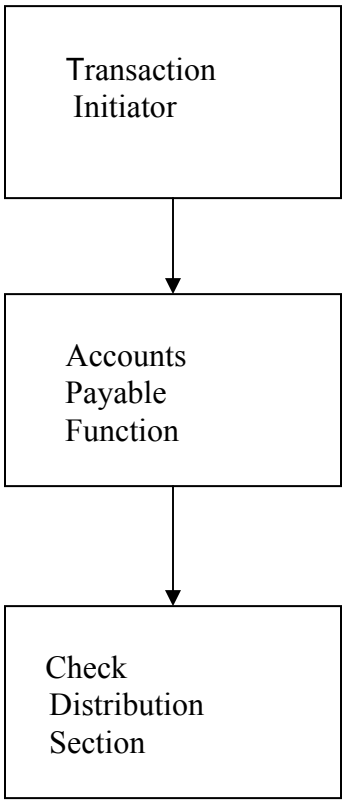
The Subtle Compromise of the Accounts Payable System

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.

The U-Turn Concept (Accounts Payable)

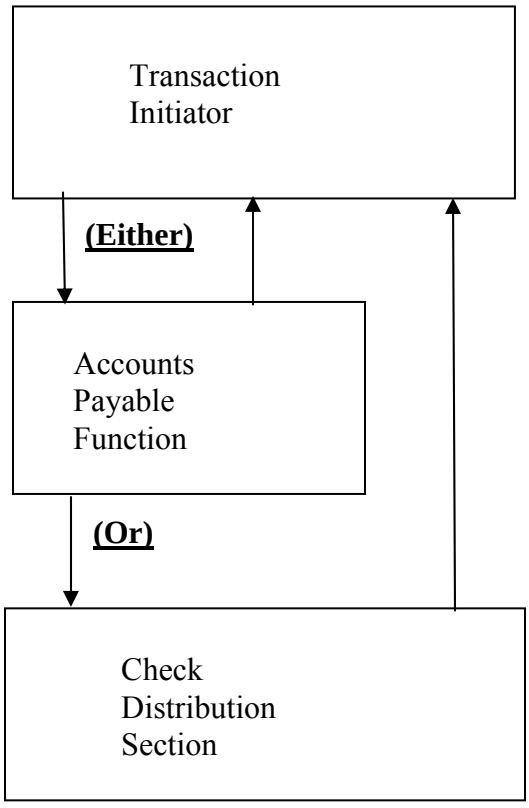
Normal Practice

(The Straight-line)



Irregular Practice

(The U-turn Concept)



Analysis of Five Disbursement Case Studies

The Washington State Auditor's Office experienced five significant fraud cases from January 1, 1996, through December 31, 2003 (eight year period of time) that involved subtle compromises of the accounts payable system and that resulted in losses totaling $1,430,271. An analysis of the **similarities** in these fraud cases resulted in the **learning objectives** included in this presentation.

Discussion of the Problems

(1) 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 disbursement fraud cases.

(2) 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 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.

(3) 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 check to them after issuance, usually so that they can hand-carry it to the vendor during a subsequent meeting.

(4) Managers should look for a "straight line" from the source requesting payment for the transaction, to accounts payable for review and production of the checks, to the individual making distribution of the checks. Anytime there is a "U-Turn" in the accounts payable function and the check is returned to the source, the transaction automatically becomes an exception transaction requiring intense scrutiny and monitoring by managers.

(5) 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. Prepare an exception report of all U-Turn transactions.

(6) The one-time payment system uses "pseudo" vendor codes and is a compromise of the internal controls over payments. It requires an exception report for these high risk transactions.

Discussion of the 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.

(2) 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.

(3) 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. Managers should periodically review the supporting documents for these transactions for trends, and examine the bank endorsements on the checks for validity. These compromises 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. Document these exceptions.

(4) Ensure accounts payable employees "process" transactions rather than "initiate" them. If accounts payable employee can initiate transactions, supervisory approval is required.

(5) Accounts payable duties should not be performed by anyone outside the accounts payable function.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

The Five Case Studies

(1) Liquor Control Board (Accounts Payable-Vendor Overpayments) ($839,707).

A freight vendor over-billed the Board and received unauthorized payments for 2.5 years. The vendor billed the Board for inflated weights on legitimate deliveries, non-existent deliveries, and duplicate or repetitive deliveries. The vendor did not bill the Board for all legitimate freight deliveries actually made during the audit period. A Board employee assigned to a position outside the freight vendor payment process (accounts payable) received and approved the vendor's billings for payment and then delivered them to accounts payable for processing. She previously worked in accounts payable and trained everyone who currently worked there. This employee also made verbal arrangements with the check distribution person to pick-up payment

checks for the vendor and then personally delivered them to him in the organization's parking lot. These actions compromised the Board's internal controls over freight vendor payments. This was a subtle compromise of the accounts payable system where the employee was able to obtain greater access to transactions than was authorized by management. However, the vendor was also not required to submit original bills for payment. In addition, 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 shipment (**fatal flaw** omitting verification of the existence of the transaction). The vendor took advantage of these weaknesses in internal controls through his relationship with the employee, and loaned her money. The agency also had a high use of "**Post-it™ notes**" by employees requesting that checks be returned to them after processing so that they could be hand-delivered to vendors. No exception records were kept, and managers did not monitor these transactions for trends. In addition, the Board was unable to find any employment contract for the freight carrier and was at a loss to explain who hired the vendor or how the vendor was hired in the first place. The Board employee finally decided to become a **whistleblower** and report the irregular activities of the freight vendor. In the end, **76 percent of all billing transactions by this vendor were false**. The freight vendor was sentenced to 57 months in the state penitentiary.

(2) Washington State Gambling Commission (Business Operations Section) ($71,750).

An Accountant issued six fictitious checks to two friends (**collusion**) and recorded them in the accounting system as refunds to valid vendors/licensees ($68,940). The employee **abused the pseudo vendor code system for one-time payments** in this scheme. He concealed these unauthorized transactions in the accounting system and on agency check registers by making the checks payable to a valid vendor called, such as "GROVE" and then by **imbedding her name in the address field for the disbursement**, such as "Tammy Grove" (i.e.; line one is the payee on the check, and lines two-four are the address of the payee). She also had been **granted too much access in the computer system**, because she was able to initiate transactions, released batches of transactions requesting that checks be produced, picked-up checks from the State Treasurer's Office, and then returned to the agency to destroy the documents and distribute the checks to her friends. There were no supporting documents created or on file for any of these unauthorized/fictitious disbursements. The Accountant also misappropriated funds from the operation of the Commission's undercover investigative unit ($2,810). The Accountant took investigative funds and agent winnings returned by the Investigative Unit Program Manager rather than depositing them in the fund or with the Office of the State Treasurer, respectively. Accounting records were falsified and destroyed to conceal these losses. This fraud scheme was detected by a bank teller when the accountant's daughter attempted to cash a $10,000 check from one of the irregular transactions rather than deposit them in her bank account. The bank's inquiry to the state agency uncovered the fraudulent disbursement. A state audit then determined the extent of the loss. The loss was less than the deductible provision of the state's insurance bonding policy ($100,000), and the private non-profit organization was uninsured. The accountant was sentenced to three months in county jail.

(3) Governor's Industrial Safety and Health Advisory Board/Washington State Substance Abuse Coalition ($144,422).

The Treasurer of the advisory board/Executive Director of the coalition processed many fictitious transactions in the checking accounts of these two organizations. There was a segregation of duties problem for this employee. She prepared and signed checks, reconciled the bank statement, and maintained the accounting records. As Treasurer of the advisory board, she issued checks to herself for reimbursement of fictitious expenses; to credit card companies for personal expenses; and to the coalition, to "cash", or to a bank for unauthorized transactions. As Executive Director of the coalition, she issued checks to pay for personal or unauthorized expenses, took payroll advances and did not deduct them from her end-of-month check, and was paid twice for the same vacation pay. This fraud was detected by the state auditor during a routine audit of the state agency. The auditor was able to follow the money from state agency disbursements to the private non-profit organization. This expanded work then detected the additional fraudulent transactions in that organization. The loss was less than the deductible provision of the state's insurance bonding policy ($100,000), and the private non-profit organization was uninsured. The employee was sentenced to 18 months in the state penitentiary.

(4) Washington State Department of Fish and Wildlife ($137,467).

The accounts payable supervisor issued checks made payable to himself and deposited them into his own personal bank account. He also issued checks made payable to vendors or lenders and **paid his own personal debts directly from the state agency treasury**. He concealed these unauthorized transactions in the accounting system and on agency check registers by making the checks payable to a false vendor called "RE:" and **imbedding his name in the second line of the address field** (i.e; line one is the payee on the check and lines two-four are the address of the payee), and by **abusing the use of "pseudo vendor numbers**" to process the transactions. The employee then volunteered to pick-up checks specifically on days he was going to receive the proceeds from these unauthorized disbursement transactions. This was not his normal duty as an accounts payable clerk. But, he verbally convinced the accounts payable supervisor that it would save her time since he was going right by the State Treasurer's Office on his way back from lunch. This was a subtle compromise of the accounts payable system where the employee was able to obtain greater access to transactions than was authorized by management. He destroyed the check registers on these same days. These disbursement transactions were charged to a balance sheet account (accounts payable) because the year-end account balance was significantly overstated. There were no supporting documents created or on file for any of these unauthorized/fictitious disbursements. Segregation of duties problem without proper monitoring of employee activities. This employee had check writing authority, including the authority to use certain codes which allowed the input of payment transactions without the creation of a supporting vendor record, was authorized to pick-up checks at the state treasurer's office, and reviewed check registers for checks issued by the agency (input and output authority). The computer system had many internal controls available which were either circumvented or not used. The agency discovered these irregularities while examining unusual adjustments to the year-end accounts payable balance. The agency found the employee's name on the redeemed

checks for these transactions during its research of the adjustments. It filed a civil suit against the employee to seize his personal assets during this case. The employee was sentenced to three months in county jail.

(5) Public Utility District No. 2 of Grant County ($236,925).

The deputy treasurer/controller processed three fictitious disbursement transactions using legitimate vendors for contracts he was able to control. The employee used "**Post-it™ notes** " to send messages to the accounts payable function instructing the staff to return the checks for these irregular/fictitious transactions to him for hand-delivery to the vendors (violation of input-output authority). This was a subtle compromise of the accounts payable system where the employee was able to obtain greater access to transactions than was authorized by management. The employee used improperly voided checks from printer set-up to issue checks made payable to himself. An optical scanner, computer printer, and color copier were used to forge the authorizing signature on the checks issued to himself that did go through the banking system, and affix false organization and bank proof of endorsements on the reverse side of the fictitious checks that never left the building. The **check redemption computer program was altered** (**true computer fraud case**), thus allowing the checks issued to himself to be accepted and processed. This is a case of **data processing functions (computer software duties) being performed in the accounting department**. The checks made payable to himself that were redeemed by the bank were then switched with the fictitious checks that had been altered to make them appear as if they had been redeemed by the bank in the Public Utility District's files after the check redemption program exception reports were intercepted, computer software changes made to accept the checks that were redeemed as if they were the fictitious checks, and then transactions were reprocessed as normal. Some documents were destroyed. Personal records were also maintained on PUD computers (ethics violation). This fraud was detected by management while investigating an unauthorized check issued to the deputy treasurer/controller which had cleared the bank. The employee was sentenced to 15 months in **Federal prison** (greater sentencing for violation of federal laws than for violating state laws).

Disbursement Fraud Concepts

The **voucher authorization and approval process** (accounts payable clerk, auditing officer, and governing body approvals) is the strength of the disbursement system in state agencies and local governments. The auditing officer function serves as an outstanding review mechanism for organization 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 check registers are high risk. These manual transactions may be shown as pen and ink changes to computer generated check registers, may

be omitted entirely, or may represent duplicate checks 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 checks must be appropriately maintained. Blank (unnumbered) checks are high risk and require an even greater level of security than prenumbered checks. Negotiable instruments (i.e.; checks) are being stolen and redeemed without the authorization and approval of the organization. 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 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 check 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 generic office supply 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 checks to the actual check register for a specified period of time (block sample). Multiple endorsements are high risk documents.

The **accounting entry for disbursement fraud** is debit expense, assets, revenue, liabilities or fund balance and credit cash.

Since disbursements fraud is recorded in the accounting system, and since the attributes of concern are "**what's too high or what's too much**". Disbursement 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 organization.

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 and Imprest Funds – The Check Fraud Risk – Bogus Checks

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.

It's important for all public organizations to understand the risk posed by bogus checks. Check fraud in the United States is a $20 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 checks have been presented to their bank for payment almost every business day.

Producing bogus 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 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 organizations have promptly detected the bogus checks during the independent party bank reconciliation process. In some cases, banks have detected the counterfeit checks when presented for payment.

In response to this risk, many public organizations have established either "positive pay" or "reverse positive pay" at their banks. This is a daily reconciliation of the 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 checks. It is extremely effective when the organization sends specific information to the bank on days when checks are issued. The bank compares the documents that come in by number and amount to a file of documents issued by the organization. If the bank has no in-file match, it contacts the organization 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 checks are then returned unpaid.

- **Reverse positive pay**. This method allows the organization to conduct its own daily matching procedures. Most banks offer customers a daily transmission of paid items that can be compared with the organization's issued check file. The organization must promptly research each suspicious document and advise the bank of items to be returned.

If a public organization 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 organizations understand the risk from bogus checks. For example, two cases have been reported where legitimate vendors created checks for an employee purchase and a delinquent loan payment.

To counter these threats, public organizations 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 organization will suffer a needless loss of funds. Organizations must:

- Notify the bank of bogus **checks** (issued in the State of Washington) within **24 hours** of redemption. One public organization has suffered a $45,000 loss because one of three bogus checks presented was not promptly identified. Another public organization identified three bogus checks 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 organization has already suffered a $26,000 loss because bogus checks were not promptly identified. Two additional schemes were quickly foiled when a public organization 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 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 organization's routing and bank account number is critical to understanding the problem. Every check a public organization issues provides all the information an individual needs to begin a bogus 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 checks with hand-held devices at or near check-cashing facilities.

We recommend all public organizations:

- Require an independent party reconcile checking 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 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 organization'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 organizations notify the bank to filter or block irregular transaction types from their checking and savings accounts, either totally or selectively.

We recommend all Office staff emphasize the information contained in this document to all public organizations during audit 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 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 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. While many managers believe that this is a dull, mundane, and perhaps even boring task, we much all change. With the "bogus" check fraud risk becoming a significant part of our life in government and our personal lives these days, the monthly bank account reconciliation is critical to stopping losses from the public treasury.

If you've ever wondered what managers should tell their employees to look for when performing the monthly bank account reconciliation, here are some of the answers from our fraud cases. Employees 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.

Other Disbursement Areas

Imprest Fund (Petty Cash) Reimbursements

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).

In addition, 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.

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 organization. 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 organization 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 organization. Original receipts should be filed with the host organization. If there is any question about documentation for such travel, contact the other organization to verify that each organization 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 organization must have an internal and external communication process that restricts access to buyers by using a central vendor reception area, and informs vendors of organization 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 organization policies and procedures. It is not a systemic issue within the organization.

Ensure the organization has policies and procedures for the control, issuance, and use of credit cards. Employees should sign an agreement indicating an understanding of the organization's policies and procedures regarding allowable uses for credit cards. Organization 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 organization 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 organization 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. Organization 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.

Employees Issue Prenumbered Checks To Cash, To Their Personal Business, Or To Themselves

The most common type of 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 organization 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 organizations 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 organization 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 organization's accounting system (i.e.; specific function or entire organization); and,(d) general disbursement accounts to carry out general organization 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 organization.

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 organization 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 organization'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 U.P. Sampson, or IBM changed to I.B. Mitchell); 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.

Town of Oakesdale Case Study ($90,256)

The Clerk/Treasurer used the Town's **credit card** for personal benefit (**mostly clothing**) and **issued checks to herself, to petty cash, or to the bank** for unauthorized purposes for 3 years. Accounting records were falsified, missing, or destroyed. The Town's loss was covered by insurance ($1 million personnel dishonesty bond with no deductible provision). The employee confessed to SAO, through her attorney, that she misappropriated public funds from the Town during the period of her employment during our interviews on June 4 and 25, 2004. Accounting records were falsified and destroyed in an attempt to conceal these irregular activities from view by Town officials and SAO. No federal funds were involved in this case. The Town's annual budget is $1 million. The loss amount averaged 3% of the Town's annual operating budget. The Clerk/Treasurer was 54 years old and had worked at the Town for 20 years.

The Schemes:

Description	Amount
(1) Used the Town's credit card for personal benefit.	$ 10,670.00

52 purchases less one credit return – August 4, 2001 thru December 22, 2003. (Collections, Inc.; Eddie Bauer; Junonia, Ltd.; LEI Lands End Clothing; Spiegel; Sunnyland Farms; Jockey.com; Petco; and, JCP Ren at Fulfill). Internet Shopping.

(2) Issued checks to herself, to petty cash, or to the bank for unauthorized purposes.	79,585.89

106 false checks – February 2, 2001 thru December 31, 2003. No supporting documents were of file for most transactions. Documents on file for vendors were false. The check register was falsified.

Total Losses	$ 90,255.89
	========

Method of Falsification of Records:

The Town's **computer was not used** to produce checks. The former Clerk/Treasurer prepared the two-part check form **manually** indicating the vendor's name in the payee section. After removing the original check from the set of documents, she used the typewriter to **change the payee** on the check from the vendor's name to the bank, to herself, or to petty cash (IBM electric typewriter correction capability). The hardest part about perpetrating a fraud of this type today is finding a typewriter to do it (i.e.; there are so few around these days).

Most of the falsified checks were **deposited** into her personal bank account. However, some were **cashed** at the bank either by herself or by two other Town employees who did not know the checks were false.

The checks from these transactions were manipulated in three ways after they were redeemed at the bank. (1) Initially, the former Clerk/Treasurer used the typewriter to **alter the payee** on the check from the bank, herself, or petty cash back to the name of the vendor shown on the original transaction. (2) Later, she **destroyed** the checks to conceal these transactions. (3) The altered check showing her name as payee was **often on file** at the Town because she **neglected to destroy the document** after redemption from the bank.

Detection Method: The **bank manager** contacted the Mayor in early January 2004 to notify him that an unknown employee was using the Town's credit card to purchase items for personal benefit. The credit card was canceled. The Town's attorney notified SAO about the loss pursuant to RCW 43.90.185. The Clerk/Treasurer's employment was terminated on January 16, 2004.

Sentencing: The Clerk/Treasurer was sentenced to 14 months in the state penitentiary.

Internal Control Weaknesses:

The Town's financial activity is handled almost entirely by the Clerk/Treasurer (**one person operation**). When the Mayor asked about decreases in the Town's "**emergency reserve funds**", the Clerk/Treasurer told him that the Town had received less funds due to the effects of the state's initiative process. This bogus statement was believed by Town officials. **No one monitored the work of the Clerk/Treasurer** to ensure that all financial transactions were authorized and for official public purposes. The Town's accounting records were in **disarray**. Most records could not be located or were destroyed. The Town Council did not believe that the falsified disbursement transactions were presented to them for approval (i.e.; concealment by showing the Council only valid transactions).

Recommendations:

The case was **referred** to the Whitman County Prosecuting Attorney. The Town should recover the loss amount and audit costs, and establish an effective system of internal controls.

Learning Objectives.

(1) **This case is a good example of all the reasons why immediately obtaining appropriate supporting documents and receipts for credit card purchases, whether made in person or via the Internet, is so important**. We have found this true in other fraud cases as well. Entities should have a clear policy for credit card purchases by employees and train staff on the required procedures. If the supporting receipts are not available at the time the credit card statement is verified, entities should immediately contact the vendor to obtain a copy of the document and then determine if the purchase was for an official public purpose. If immediate action is taken, the entity will usually be able to obtain the supporting receipts for the transaction. Employees should be disciplined at the level determined appropriate for the action. For example, the entity could provide a verbal reprimand for the first offense, a written reprimand for the second offense, and then terminate credit card privileges. However, **if the entity does not promptly obtain the supporting receipts for the transactions, it may be impossible to obtain them later**. And, we have similar results even when sending subpoenas to the vendors to obtain the required information for us to make a determination about the official public purpose of credit card transactions. Most Internet vendors are located out-of-state and do not respond favorably with the information we need, if at all, even when using our subpoena power. The reason is that our administrative subpoena "Duces Tecum" cannot be enforced outside the State of Washington. So, a word to the wise should be sufficient – **get supporting documents immediately or suffer the consequences we faced in this fraud case** (i.e.; inability to obtain the support needed to prove that purchases were for official public purposes or for personal purposes).

(2) **This case is also a good example for entity managers about the importance of paying all bills on time (i.e.; once a month after presentment of the statement)**. When there were supporting documents for some of the fictitious disbursement transactions in this case, they were actually false. The actual vendor statements on file were original documents, but they represented a false condition (i.e.; **false originals**). If monthly bills are paid promptly, entities receive only one statement per month from each vendor. When bills are not paid on time, vendors often send additional "reminder" or "late payment" statements to the entity. These "additional" statements, while valid original source documents, were false representations of the amount due on the account. The Clerk/Treasurer took advantage of this situation and used the "extra" statements to support the fictitious checks issued in this case. For example, **there were almost 20 monthly payments to the utility company each year**. While 12 monthly payments would be our normal audit expectation for this vendor, each of these payments was supported by a monthly vendor statement. If we asked the vendor for a payment history record, we would find that only 12 (or less) of the monthly payments went to the vendor. The remaining payments represented fictitious transactions where the Clerk/Treasurer subsequently altered the payee on the check to herself and then deposited the check into her personal bank account.

Reverse Engineering and Computer Assisted Audit Techniques (CAATs).

Once we know how a fraud was perpetrated, we should be able to identify the attributes in the case that we could test for, such as by using CAATs, to identify the false disbursements in this fraud case. This is called "reverse engineering". Analyzing the final results of the case, we find that **there were way too many monthly payments per year to at least three vendors**. They

were: (1) The name of the Clerk/Treasurer; (2) Petty Cash; and, (3) the utility company. With this answer, we now know that we must perform a simple CAATs test using the expenditure data base to **identify all vendors with more than 12 monthly payments per calendar/fiscal year**. Since our expectation for most vendors is that there should not be in excess of 12 payments per year, this CAATs test would give us the universe of vendors with an unreasonable level of activity. Once a vendor is identified with questionable activity, we must then review the underlying supporting documents to determine whether all disbursements were made for official public purposes.

For example, our expectation for any entity should be that **there are normally 12 monthly payments for all types of utilities** (i.e.; electric, telephone, gas, water, sewer, propane, garbage, etc.). And, if we frequently make purchases from other vendors, we similarly would expect to find 12 monthly payments for each of these vendors as well. Anything less than 12 payments normally would not be a problem. And, sometimes there would be extraordinary circumstances where there would be 13 payments or more per year. But, when the level of activity reaches approximately 20 monthly payments, this is cause for concern. Our response to this condition is to test the underlying supporting documents to determine whether all disbursements were made for official public purposes. This testing could include an inquiry to the vendor to obtain a copy of the entity's payment history for the audit period under review.

The tables below present the test results for the number of payments made to the three vendors cited in this fraud case.

Table Number 1. This table indicates the number of payments the Town made to each of these vendors according to the information actually recorded on the check register and in the accounting system.

Vendor	CY 2003	CY 2002	CY 2001 (6 Months)
Clerk/Treasurer	31	35	26
Petty Cash	19	24	18
Utility Company	18	17	8

Our analysis of these transactions absolutely detects the fraud. Our actual results are shown in the following table.

Table Number 2. This table is the actual number of payments the Town made to each of these vendors based upon the actual check count during this audit.

Vendors	CY 2003	CY 2002	CY 2001(6 Months)
Clerk/Treasurer	60	55	42
Petty Cash	41	35	27
Utility Company	9	11	8

Remember that when fictitious disbursement transactions are created, the payee vendor must be recorded on the check, even if it's wrong (including an entry for a blank payee). Fraud perpetrators usually establish a pattern for the irregular activity. And, if the level of fraudulent activity is significant, we should be able to identify the pattern by using this simple CAATs test, such as in this audit example.

Additional CAATs Tests for Disbursements.

There are a multitude of CAATs tests available for use when performing analytical procedures on the entity's disbursement data base. The following list is provided for your consideration:

- Vendor summary multiple year trend, sorted highest to lowest. Scan for unusual vendor names, unusual amounts in relation to vendor names, and increasing activity.

- Vendor summary multiple year trend within an account code category (such as supplies, travel, or other risky area). This identifies unusual vendors given the category, unusual levels, and increasing trends.

- Vendor summary for credit cards. This identifies increasing activity levels and new cards. Drill down to transaction descriptions (if available) to review for unusual activity.

- Negative transaction activity. Unusual activity levels might indicate over-payments. It could also suggest weak voucher processing controls.

- Duplicate payments. Scan for unexpected double payments. Due to volume, generally limit scope based on $$ amount and/or timing of duplication. Also scan for duplicates representing regular payment activity for anything unexpected or unusual.

- Employee versus vendor match (based on address and last name) with employee payroll total and vendor payment total. This generally identifies travel expense. But, there is a potential to identify fraudulent vendors. Including the amount helps to focus the review.

- Vendor duplicate address. This test will most likely identify vendors where payments have been split with potential purchasing/bid law consequences. It also has the potential to identify fraudulent vendors.

- Vendor validity testing (based on Social Security Account Number, for example). This is particularly useful for claims benefit systems, pensions, insurance pools, etc.

- Expenditures by journal or system code. This can identify smaller systems which may reflect higher risk, such as manual checks.

Part Four: Understanding 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.**

The most common payroll fraud involves an individual who receives more pay than authorized. They simply issue too many checks to themselves for too much money, checks to themselves for work not performed, or make unauthorized vacation buy-outs for themselves. The fraud can involve normal payroll, overtime, or vacation and sick leave. The question is: "How much money is the employee supposed to make, and did they exceed that amount".

The prime suspects are employees performing payroll duties and department timekeepers who falsify their own payroll after approval by a supervisor.

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.

The U-Turn Concept (Payroll)

Normal Practice (The Straight Line Concept)	Irregular Practice (Fraud – The U-Turn Concept)
SOURCE (Individual)	SOURCE (Individual)

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 check). 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 checks 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 organizations, 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 checks to the actual check register for a specified period of time (block sample) for agreement. **Multiple endorsements** on payroll checks 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 check 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 check registers. These manual transactions may be shown as pen and ink changes to computer generated check registers, may be omitted entirely (i.e.; gaps in the check numbers listed), or may represent duplicate checks previously processed through the system. Governing bodies may not even approve these transactions if the unauthorized checks were omitted from the check registers.

Payroll Fraud Statistics
Washington State Auditor's Office
January 1, 1987 through July 31, 2006

Category	Number Of Cases	Amount Of Losses
Mid-Month Payroll Draws	6	$ 48,009
False Overtime and Stand-by or Call-Back Time	8	379,610
COBRA Manipulations	5	58,759
Payroll Office Manipulations	8	108,860
Payroll Abuse by Managers	5	113,146
Employee Time and Attendance	53	243,646
Total Payroll Fraud Cases	85	$ 952,030
Percentage of Total Fraud Cases	11.6%	7.3%

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.

The Five Most Common Payroll Fraud Schemes

(1) **Ghost employees (few)**.

Attributes: (a) Employee never comes to work. (b) Time sheet is not signed by employee. (c) Dual endorsements on payroll checks.

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. To detect frauds of this nature, consider reviewing all payroll cards or timesheets for one pay period to identify all payroll cards or timesheets that are not signed by the individual (i.e.; supervisory approval only). These are high risk transactions which could represent ghost employee situations and all payroll cards or timesheets that are signed only by the individual (i.e.; no supervisory approval).

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 Study: Tacoma School District – over $114,000

The largest ghost employee case in the state of Washington involved the district's transportation director who hired 13 ghost employees to perform bus monitor duties on transit busses the district used when its bus drivers were on strike. While the employees had official files in the human resources department, they never came to work. The transportation director approved their unsigned time sheets, obtained their pay check from the payroll department, and split the proceeds with the individuals. This case is a good example of the U-Turn concept in the check distribution section. The fraud was detected by the police department. The director pistol-whipped an uncooperative co-conspirator who told the police about the fraud from his hospital bed. The case was reported in the local newspaper and was then investigated by the state auditor's office. After learning about this fraud case, the state auditor's office investigated the matter. Losses exceeded $114,000 over an eight year period of time. The loss was covered by the district's insurance bonding policy. This is a very old case and sentencing information is not currently available.

(2) **Mid-month payroll draws not deducted from end-of-month payroll (few)**.

Attributes: (a) Occurs in small organizations. (b) More than one payroll draw per month. (c) Blank, void, or loss-leader 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 check. 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 check was a "void" or by indicating an incorrect amount for the transaction. In one case, unnumbered (blank) checks 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.

(3) **Unauthorized employee pay (many)**.

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 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 organizations, 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.

Case Study: University of Washington Medical Center – over $264,000

The largest payroll fraud case in the state of Washington occurred because an employee submitted his own time sheet without approval by his supervisor. 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 (i.e.; time sheet not signed to approve it). This fraud was detected by employees in the payroll department. The employee visited the payroll department and asked if he could take a payroll action to pay his employees for other things. When advised this violated University policies and procedures, the employee left while mentioning that he would find a way to take care of this situation. This concerned the payroll department who subsequently reviewed the employee's time records and discovered the fraud. This loss was covered by the University's insurance bonding policy except for the $100,000 deductible provision. The employee was sentenced to one year in the state penitentiary.

(4) **COBRA program abuses (few)**.

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 checks 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 (few - none in Washington – yet)**.

Attributes: (a) Payroll checks are issued prior to pay date. (b) Payroll 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.

Prevention/Detection: Review the bank endorsement of the check for withheld funds to determine if the check was deposited into the proper bank (one will do). If the check was deposited into the correct bank, there is no problem. If the check was not deposited into the correct bank, such as a personal bank account of a key employee, then there is a problem.

Case Study: Private Sector Business (Unknown Loss Amount)

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.

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 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 checks 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.

Key Learning Objectives for This Class

(1) The attribute of completeness is critical to understanding the risk for fraud. What is the universe of high risk transactions that all managers must periodically monitor?

(2) Always seek (or prepare) computer-generated exception reports to identify the universe of known high risk transactions, such as:

(a) Accounts receivable write-off transactions.

(b) Accounts payable.

(1) U-Turn transactions (Post-it™ notes).

(a) Accounts payable function.
(b) Check distribution section.

(2) Pseudo vendor codes (abuse, then fraud).

(c) Payroll U-Turn transactions (at supervisory position).

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