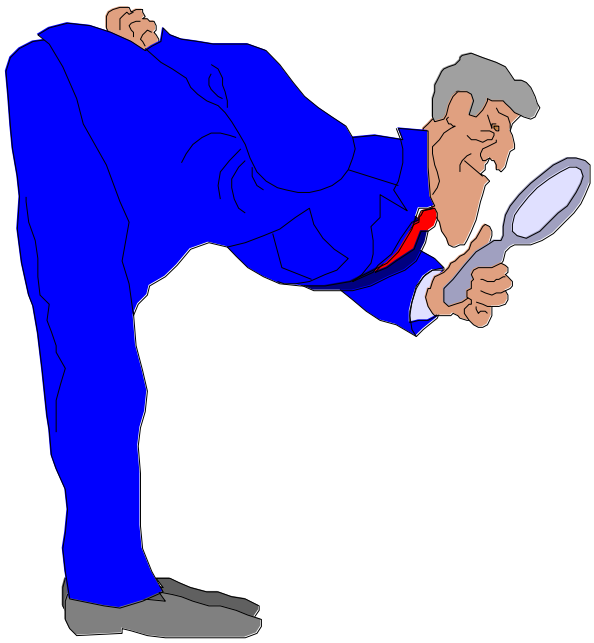


Internal Controls And Fraud

(Current Hot Topics and Fraud Risks About Employee Embezzlement in the Workplace)

Presented to: Association of Washington Cities
Annual Conference
Spokane Convention Center
Spokane, WA – June 22, 2006

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

BIOGRAPHY

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

Joe is the Audit Manager for Special Investigations at the Washington State Auditor's Office where he is responsible for managing the agency's Fraud Program. He specializes in employee embezzlement fraud within all state agencies (170) and local governments (2,400) in the state of Washington. He monitors all fraud audits throughout the state and has participated in the investigation of almost 700 cases involving losses of over $12.8 million in the past 19 years.

Joe received his Bachelor of Science Degree from the University of Tampa (Florida) in 1963 with majors in both accounting and business administration. He completed graduate studies at Air University, Maxwell Air Force Base, Alabama, in Comptrollership (1975) and Military Science (1977). He is a Certified Fraud Examiner (CFE), a Certified Internal Auditor (CIA), and a retired United States Air Force Lieutenant Colonel. His audit experience includes 20 years with the Air Force Audit Agency and 22 years with the Washington State Auditor's Office.

Joe is the fraud audit training instructor for the Washington State Auditor's Office, and the author of the agency's "Fraud Audit Manual", and the following agency training courses: "Fraud Detection and Development", "Fraud Auditing Update", "Computer Fraud", "Cash Count Procedures", and "Interviewing Techniques". He received the agency's "Outstanding Employee Award" 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 fraud award is similar to the Pulitzer Prize in the field of Journalism. In 2004, the membership elected him to be the Vice-Chair of the Board of Directors of the Association of CFEs, one of the highest positions any CFE may hold in the profession. Joe is a Life Member, Fellow, Regent Emeritus, and was an adjunct faculty member and 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", "Cash Disbursement Frauds -- Treasury Funds Are The Target", "All Wired Up -- Electronic Funds Transfers are Prime Fraud Targets", and a regular "By-Line Column on Fraud's Finer Points" have been published in *The Fraud Magazine*, the Association's international journal. He is also the founding and current President of the Pacific Northwest Chapter of the Association, and is a frequent speaker at chapter fraud seminars and conferences.

Joe writes "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 its "Internal Controls Checklist".

Joe presents fraud awareness seminars to over 3,000 auditors and management officials of governmental entities and professional associations in North America each year.

Plan For Success

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 cash 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. **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 cash 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 case 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 STATISTICS

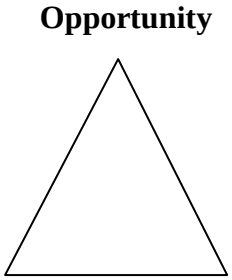
State of Washington
January 1, 1987 through December 31, 2005

CALENDAR YEAR	NUMBER OF CASES	LOSS AMOUNTS
1987	32\	$ 388,936\
1988 \ 6 Year	26 \	451,122 \
1989 \ Average	31 \ 23	358,654 \ 301,582
1990 /	15 /	120,121 /
1991 /	15 /	264,027 /
1992/	20/	226,629/
1993	18	642,439
1994	30	903,304
1995	37	689,080
1996	48	958,805
1997	33	1,540,368
1998	31	597,479
1999	42	1,047,113
2000	30	167,363
2001	68 **(Note)**	484,060
2002	56	1,122,328
2003	62	2,253,394
2004	47	331,803
2005	57	258,960
19 Year Total	698	$12,805,985 (Average = $18,347)
19 Year Average	37	$ 673,999 (Doubled +)
	===	=========

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

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.

<u>The third leg of the triangle</u>.

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-off's) 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 cash 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 cash disbursement frauds.

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

Primarily prepares customer accounts receivable billings, cancellations and adjustments (write-off's), 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:

Comes to work early or leaves late.

Works nights and weekends.

Is seldom missing from the office, even to take leave or vacation.

Reports to the office during brief absences (one day or less), by telephone or in person.

Asks others to hold their work for them without processing it until they return.

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

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

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

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

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

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

Employees who brag about recent gambling winnings or family inheritances.

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

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

Cashiers who always balance and are never over or short.

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

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

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

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

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.

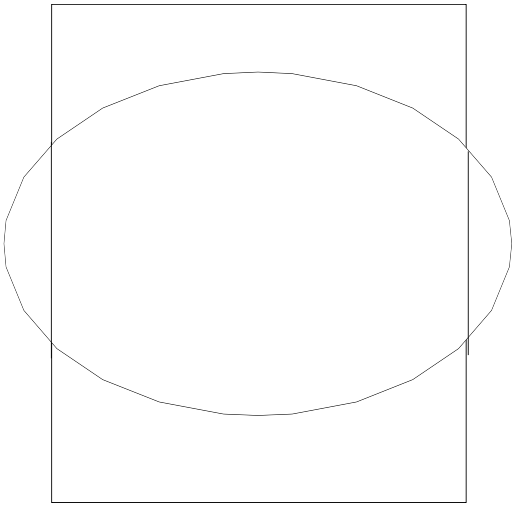
What fraud perpetrators do -- **They simply don't play by the rules**. They do the following:

Ignore internal controls established by management.

Compromise internal controls established by management.

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

The circle/square concept (Example):



- The "circle" represents the internal control procedure involved, such as making organization bank deposits on a daily basis.

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

Critical Fraud Risks

(1) Lack of monitoring of employee tasks by managers.

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.

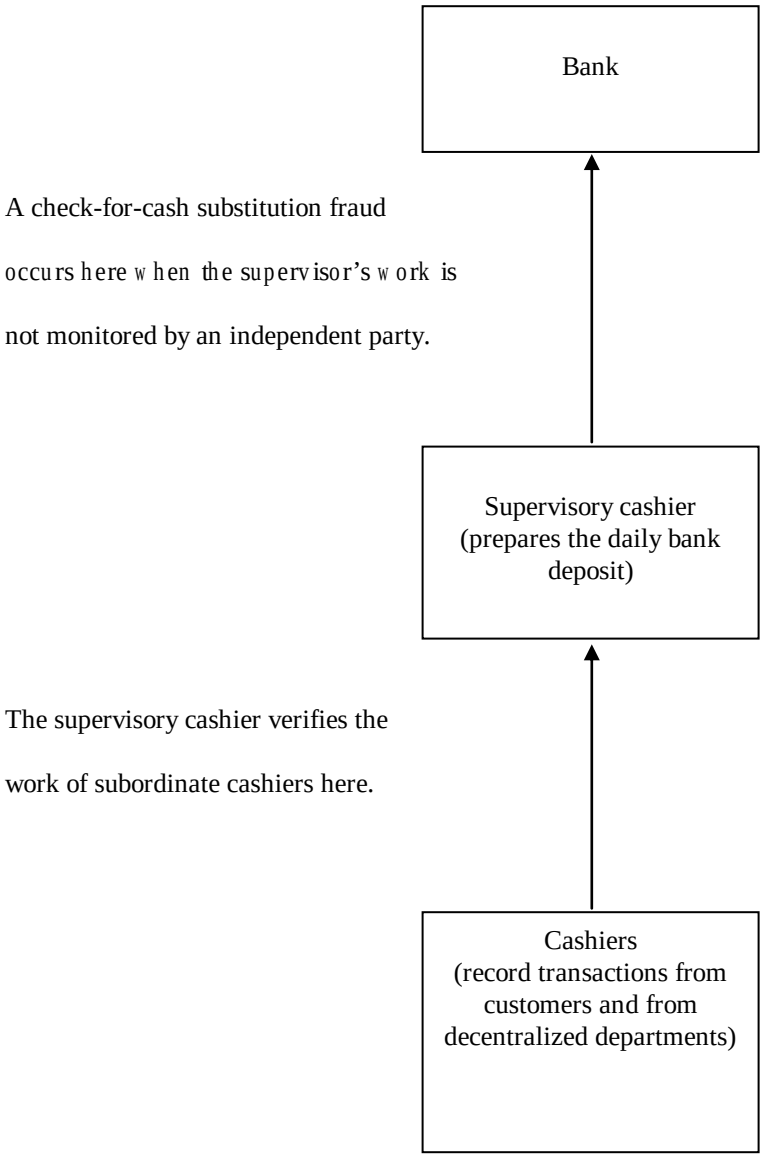
- If you have on-line banking capabilities for the depository bank account, verify the check and cash composition of the actual bank deposit from the bank's records. Copy the bank deposit slip to provide evidence of this monitoring action.

- 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



(2) <u>The subtle compromise of the accounts payable system</u>.

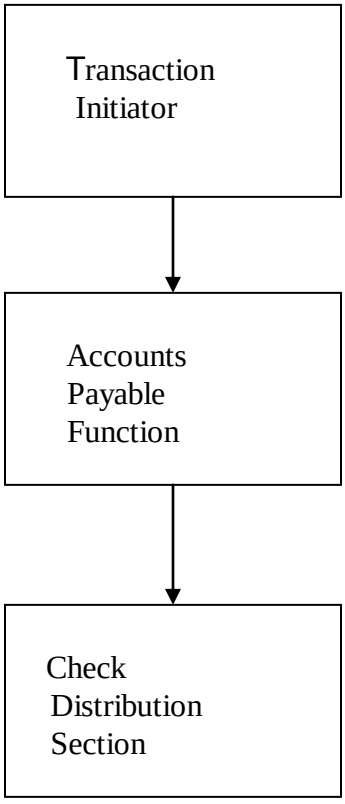
The ultimate objective of any cash disbursement scheme is a check issued by the organization which is then converted to cash for personal gain.

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.

The U-Turn Concept (Accounts Payable)

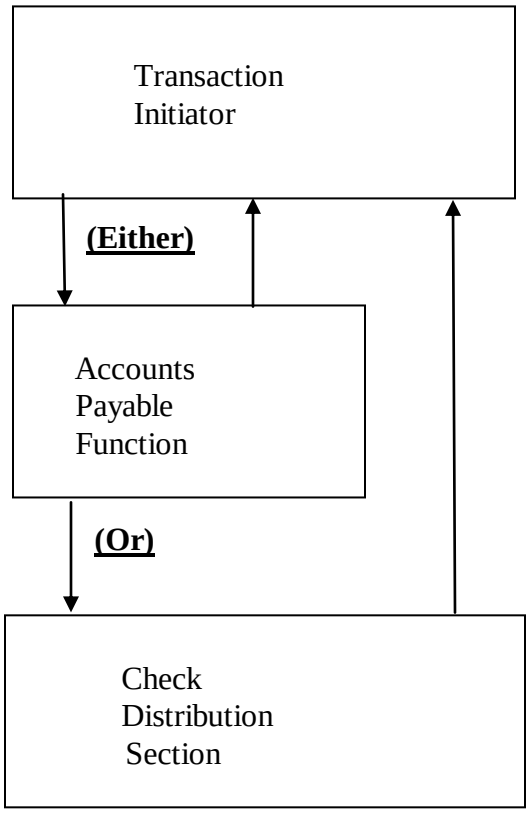
Normal Practice

(The Straight-line)



Irregular Practice

(The U-turn Concept)



The Washington State Auditor's Office experienced five significant fraud cases from January 1, 1996, through December 31, 2003 (eight years) that involved subtle compromises of the accounts payable system resulting in losses totaling $1,430,271. This presentation includes the learning objectives from these fraud cases.

Problems:

The ultimate objective of any cash disbursement scheme is to obtain a negotiable instrument and subsequently convert it to cash for personal gain. Managers often think that the check issuance process is unimportant. After all, it's just paper.

(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 cash 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 cash disbursement fraud cases. Thus, they are able to create fictitious disbursement transactions using either legitimate or false vendors, obtain the check and then use the proceeds for their own personal benefit.

(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.

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.

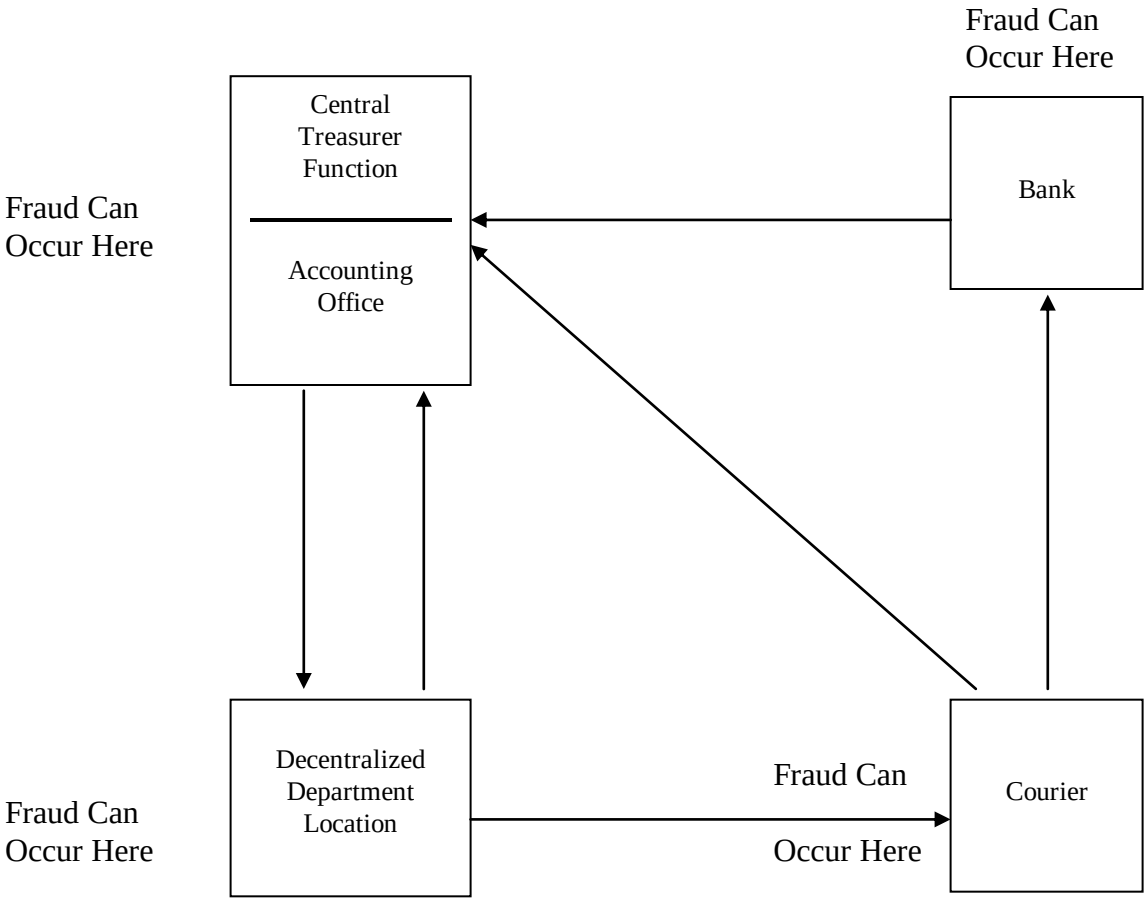
Routine Fraud Risks

(1) Lack of fixed responsibility for funds.

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. 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?"

Cash Receipting Flow Chart – Decentralized Departments



Decentralized Cash Receipting Flow Chart – 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**)

(2) Bogus Check Fraud Risk.

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 **warrants** (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 warrants presented was not promptly identified. Another public organization identified three bogus warrants promptly and avoided a $450,000 loss.

Notify the bank of bogus **checks** within **30 days** of the bank statement date. However, performing the bank reconciliation immediately upon receipt is preferred. One public 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 warrant accounts daily and checking accounts immediately upon receipt of the bank statement.

Include either positive pay or reverse positive pay procedures in banking agreements.

Ensure check stock is designed to meet industry standards and has a sufficient number of security features that make counterfeiting more difficult.

(3) Money laundering of stolen organization revenue and disbursement checks.

For the purpose of this discussion, "*money laundering*" is the process employees use to negotiate

stolen revenue checks in order to obtain the proceeds for their own personal benefit. These checks represent legitimate payments made by customers for a service provided by the government. These funds should be in your Treasury.

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 $20 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.

(4) Accounts receivable.

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

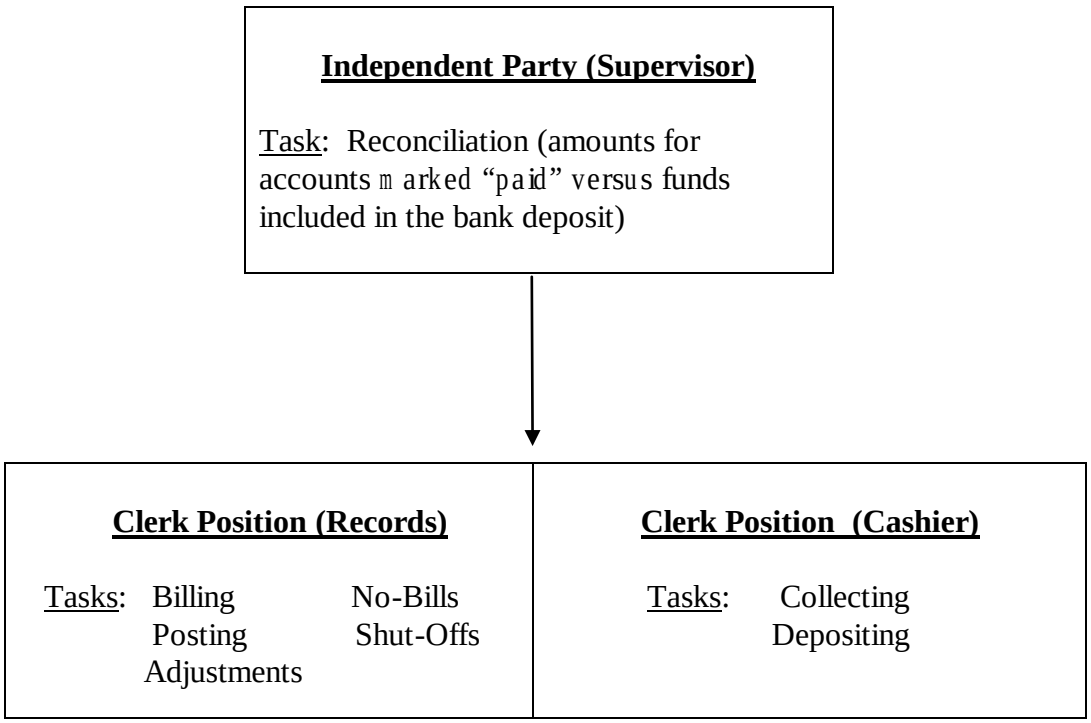
Accounts Receivable – Internal Control Structure - Duties of Personnel

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, 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.

Summary of Major Areas of Concern in Accounts Receivable Systems

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

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

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

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

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

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

(5) <u>Payroll</u>.

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.**

<u>The Fraud Perpetrator</u>:

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).

<u>All Employees</u>. 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.

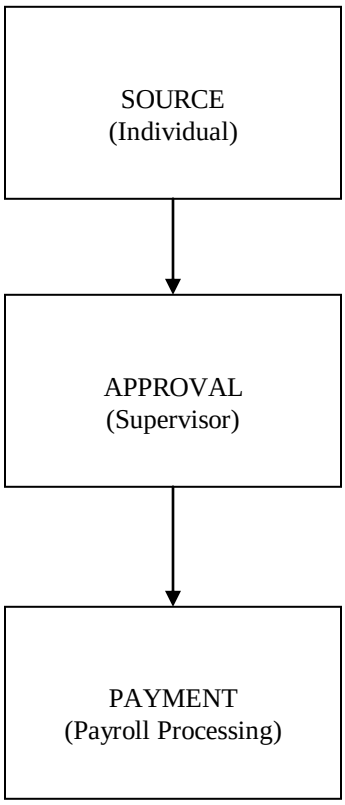
<u>Payroll Department</u>. Employees in the payroll function falsify organization accounting records to conceal unauthorized transactions.

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)

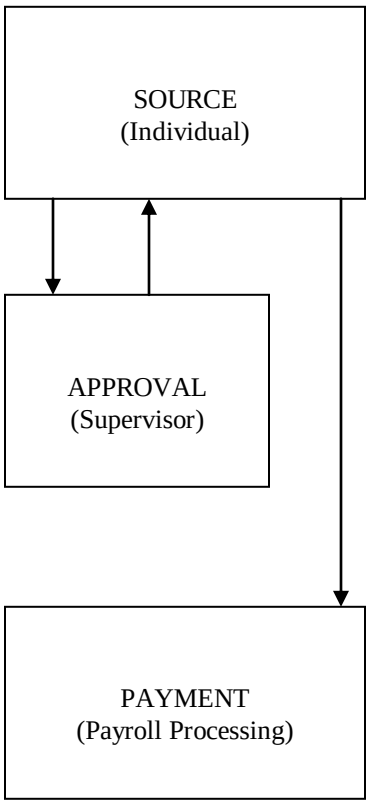
Normal Practice

(The Straight Line Concept)



Irregular Practice

(Fraud – The U-Turn Concept)



PAYROLL FRAUD CASES

State of Washington
January 1, 1987 through December 31, 2005

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	52	240,627
Total Payroll Fraud Cases	84	$ 949,011
Percentage of Total Fraud Cases	12.0%	7.4%

THE FIVE MOST COMMON PAYROLL FRAUD SCHEMES

(a) **Ghost employees**. (Few cases.)

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

High risk employees: (a) Part-time, seasonal, or temporary employees. (b) Employees who terminate employment at the organization.

Prevention/Detection: Use a payroll list and visit Departments to verify existence of employees. Observe employee work stations or ask an employee who does not normally perform payroll duties.

(b) **Mid-month payroll draws not deducted from end-of-month payroll**. (Few cases.)

Attributes: (a) Occurs in small organizations. (b) More than one payroll draw per month. (c) Blank, void, or loss-leader warrants/checks are used for the unauthorized transaction. (d) An unauthorized adjustment must be processed, usually at the end of the month, to record the extra payment in the accounting system.

High risk employee: (a) Payroll Department employee or manager.

Prevention/Detection: (a) Review the payroll record of Payroll Department employees and managers. (b) Review the number of payroll payments per employee per month.

(c) **Unauthorized employee pay**. (Many cases.)

Attributes: (a) Fraud is usually not systemic. (b) It's a specific employee who manipulates their own payroll records.

High risk employees: (a) Department timekeepers. (b) Department managers. (c) Payroll Department employee or manager.

Prevention/Detection: (a) Monitor payroll records for key employees. (b) Review payroll records for unusual patterns for overtime, stand-by time, call-back time, regular hours, compensatory time, sick leave, and annual leave. (c) Look for a straight line from source to approval to payment. (d) Determine whether the organization has and properly uses compensatory time for employees. Transactions must be recorded.

Prevention/Detection: Determine if payroll checks/warrants are negotiated/cashed prior to pay date or by an unauthorized individual by reviewing endorsement information.

(d) **COBRA program abuses**. (Few cases.)

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.

(e) **Advance release of withheld funds**. (Few cases – none in Washington, yet.)

Attributes: (a) Payroll warrants/checks are issued prior to pay date. (b) Payroll warrants/checks are endorsed prior to pay date and by an unauthorized individual.

High risk employees: (a) Payroll Department manager. (b) Chief financial officer of the organization.

Prevention: Review endorsements on tax withholding checks.

Key Learning Objectives for Today

(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 government, particularly after internal control weaknesses have previously been the subject of audit reports.
- The best defense against fraud is a good offense (for both deterrence and detection purposes). This is where an ounce of prevention is better than a pound of cure.
- The challenge is to go back to work and monitor something (anything).
- Awareness that fraud can (and does) happen is the key to detection.