

***Risk Factors And
Red Flags For State
Auditors***

AUTHOR'S BIOGRAPHY

Jerry E. Spratt, CFE, CPA, CFF, CFCI, CFSA, CGFM

Jerry E. Spratt is the Assistant Legislative Auditor for the Arkansas Division of Legislative Audit, serving the organization for 37 years. He received his BA in Business and Economics from Hendrix College, Conway, Arkansas, in 1971 and his MBA from the University of Central Arkansas, Conway, Arkansas, in 1972.

Mr. Spratt directed the fraud deterrence and detection efforts of the Division between 1980 and 2007. These efforts include the investigation of hundreds of governments in Arkansas, obtaining over 200 confessions and assisting State Prosecuting Attorneys in the successful prosecution of over 200 criminal cases with only one felony not guilty verdict.

Mr. Spratt is a member of the; the Association of Certified Fraud Examiners, currently serving on the ACFE CPE Committee and as President of the Arkansas Chapter; American Institute of Certified Public Accountants and serves as a CPA Ambassador; Arkansas Society of Certified Public Accountants, serving on its Professional Ethics Committee, Policy Committee and the Board of Directors; Association of Financial Crimes Investigators; and many other professional organizations. He also chairs the Investigative Audit Subcommittee of the Southwest Intergovernmental Audit forum.

Mr. Spratt conducts seminars at national conferences and for others on the subject areas of forensics, risk analysis, fraud investigation, deterrence, prevention and detection; internal controls; interviewing, interrogation and confessions; trial preparation; expert witness testimony; report writing; Risk Suite, SAS 99 & 112; and SOX and PCAOB Audit Standard 5.

He is the Chairman of the committee responsible for scheduling CPE for the Arkansas Society of CPAs Fraud Conference. He is the Arkansas Society of CPAs Oversight Board Member – Continuing Professional Education Task Force.

Mr. Spratt is Secretary and past Chairman of the Board, Treasurer past Chairman of the Supervisory Committee (audit committee) of the Arkansas Federal Credit Union (AFCU), a 725 million dollar financial cooperative. He received the Association of Certified Fraud Examiners' 2004 CFE of the Year award, the Arkansas Society of CPA's 2004 Outstanding CPA in Government award and the Society's 2005 Mac Angel Discussion Leader of the Year award.

Risk Factors and Red Flags For State Auditors

Table of Contents

I.	Introduction	1
II.	Fraud Risk Analysis Tools	3
III.	Fraud Investigation Tools	5
IV.	Interviewing	7
V.	Other Investigative Techniques	12
VI.	Evaluating and Investigating Fraud Risk	14
VII.	Investigator Traits	16
VIII.	Relevant Assertions	17
IX.	Investigating Cash Receipts	19
X.	Cash Receipt Risk Factors and Red flags	21
XI.	Other Risk Factors and Red Flags	39
XII.	Summary	41
	Bibliography	43

© 2009 FraudBusters, Inc.

This material is designed solely for the participants attending this program. No portion of this material may be reproduced, copied or transmitted to any other person without the express written consent of FraudBusters, Inc.

Chapter I

Introduction

The purpose of this manual is to inform State Auditors of the various subject matters employees need to be taught to be effective fraud investigators. If State Auditors equip these employees with the knowledge recommended in this course, the employees' value to State Auditors should be substantially enhanced. Many frauds should be detected during the course of routine audits of state governments.

Occupational Fraud Types

The nine occupational fraud types are listed as follows:

- Cash larceny – theft of recorded revenue
- Skimming – theft of unrecorded revenue
- Payroll fraud – unauthorized salary payments, withholding fraud, ghost employees and workers compensations fraud.
- Employee reimbursement fraud – inappropriate reimbursement to employee for personal purchases, false purchases and inflated purchases
- Check tampering – fraudulent altering of any part of a check
- False billing – unauthorized personal payments or charges to credit or purchase cards, intentional overpayment schemes and false vendor schemes

- Other asset fraud – theft of other assets
- Corruption – kickbacks, conflict of interest schemes, bid-rigging, illegal exaction and illegal gratuities
- Financial statement fraud – fraudulent misreporting of financial statements

Examples of specific types of occupational fraud schemes are as follows:

- Ponzi scheme – pyramid false investment scheme
- Lending scheme – unauthorized loans to inappropriate individuals and loan documentation falsification and
- Asset flip scheme – asset inflation scheme designed to defraud a lender

Chapter II

Fraud Risk Analysis Tools

The investigator utilizes the following tools to assess the risk of fraud:

- ***Observation***

Observation is used to gather information not available through other means or to confirm information obtained through other risk analyses. Observation is used to assess compliance with policies, procedures, and internal controls. Observation may reveal a deficient control environment including a lack of ethics and integrity on the part of top management.

- ***Inspection***

The inspection of records and recorded transactions may reveal red flags or indicate a high risk of fraud. Searching for large journal entries in round dollar amounts at or near the close of accounting periods is an example of an inspection procedure.

- ***Interviews***

Interviews reveal information not available through other means or confirmation of known information. Through interviews, investigators may note changes in management

and employee behavior indicating deception, corruption, red flags, and other abnormal occurrences that indicate fraud.

- ***Analytical reviews***

Analytical reviews involve comparing financial information from period to period. The analysis may be horizontal or vertical. Reviews may reveal abnormal financial data relationships. An example could be a sudden, unexplained increase in revenue that could indicate inappropriate revenue inflation.

- ***Walk-throughs***

A walk-through involves tracing an original source document through the recording processes. A walk-through is designed to test the reliability of the internal control systems, and therefore, discover opportunity points of fraud execution.

Chapter III

Fraud Investigation Tools

The investigator utilizes the following tools to detect fraud:

- ***Observation***

The investigator may observe the fraud execution or concealment through normal on-site activities, stake-outs or cameras.

- ***Inspection***

Inspection of records and transactions is used to verify the authenticity of recorded transactions and events. The investigator must be alert to destroyed, missing, falsely created, altered, and duplicated documents and false journal entries.

- ***Interviews***

Interviews are used to eliminate suspects, gather information that is only available through interviews, confirm already determined facts and identify the fraudster. During the interrogation process, interviews should be conducted starting with the least likely suspect progressing to the most likely suspect. This allows the interviewer to gain all available information before confronting the primary suspect in an interrogation.

However, if the investigator is concerned about other interviewees alerting the fraudster

to the investigation, the investigator may decide to rely on information from all sources other than interviews prior to interviewing the fraudster.

- ***Confirmations***

Confirmations are used to independently verify information. Common forms of confirmations may be used to verify bank, investment, accounts receivable, liabilities, revenue, expense, customer, vendor, taxpayer, and donor information.

- ***Recalculations***

Recalculations are used to verify computations used in accounting entries and involve the investigator recalculating the data for verification purposes. A common procedure in County audits is to re-compute the final distribution of tax collections to all taxing units.

Chapter IV

Interviewing

The goals of an interview should be to determine the truthfulness of the interviewee and manage the behavior of the interviewee. The three types of interviews are professional interview, SAS 99 interview, and admission-seeking (interrogation) interview.

A brief discussion of each type follows.

- ***Professional interview***

The professional interview is conducted to obtain information that is not available through other means or to verify information obtained through other investigative techniques. The professional interview is not designed to obtain a confession. The three types of professional interviews are directive, nondirective and combined.

Directive

The investigator uses the directive interview to exercise more control over the interviewee's responses. Closed-end questions are asked in the controlled interview. A closed-end question is answered yes or no. An example of a closed-end question is, "Did you receipt all funds on June 1?" If the interviewee is circling, providing responses not pertinent to the question, the directive approach should guide the interviewee to respond to the question.

Nondirective

The nondirective approach is used to encourage the interviewee to provide complete information concerning the questions. Open-ended questions are used in the nondirective approach. An example of an open-ended question is, “Explain the Treasurer’s Office receipting and depositing process?”

Combined

The third type of interview is the combined interview. This approach switches between the directive and nondirective. It consists of both closed-end and open-ended questions and is used to more closely control the interview at times and to seek maximum information at times.

The only tools the investigator has to manage the behavior of the interviewee are the types of questions asked, the selection of the evidence to discuss, and the investigators body language.

Investigators need to be knowledgeable of the various types of questions to ask. The first type is a general question which is used to establish rapport. If the investigator does not establish rapport with the interviewee, the interview will most likely be unsuccessful. An example of a general question is, “How long have you been working for the organization?”

The second type is a follow-up question. These questions are used to further investigate information provided by the interviewee. They should be used when the investigator determines deception on the part of the interviewee.

The third type is a secondary question which is used to encourage continued response from the interviewee. There are two types of secondary questions, i.e., attentive echoes and summary returns. Attentive echoes are interviewer responses like, “OK, I see, yes” and also consist of the interviewer nodding his head to show signs he understands and agrees with the interviewee’s response. Summary returns are used to summarize and solidify the interviewee’s response. The investigator summarizes the interviewee’s response and asks the interviewee to confirm the summary is correct.

The fourth category consists of tie downs and tags. These are used to solidify the interviewee’s response. Tie downs are asked at the beginning of the question and consist of, “Wouldn’t you agree, isn’t it true.” Tags are added at the end of a question. An example of a tag is the word, “correct?”

The fifth question type is a leading question. These questions are used to confirm the interviewer’s assumption while directing the interviewee’s attention to the question portion of the inquiry. An example of a leading question is, “Mr. Smith, I assume that when Ms. Buggsy is not available, you sign her name to the Street Fund checks and she

never sees the checks until she does the bank reconciliation, correct.” The interviewer is seeking confirmation that Smith signs Buggsy’s name to the checks when Buggsy is not available but directs the interviewee’s attention to the question portion of the inquiry, “she never sees the checks until she does the bank reconciliation, correct?”

Investigators must be able to recognize behavioral symptom changes because they indicate deception on the part of the interviewee. The symptom changes may be verbal or nonverbal. Verbal symptom changes consist of truth reinforcement, voice changes and tentative responses. Nonverbal symptom changes are recognized as non-normal physical interviewee activity, e.g., hair twisting, leg and arm movement, touching nose, posture changes, eye contact, etc.

Nonverbal symptom changes are more reliable than verbal changes. The investigator should look for behavioral symptom clusters, i.e., two or more behavioral symptom changes. The changes must occur after the interviewee asks the question. Before the investigator can recognize the changes, the interviewee’s behavior must be “normed.” The investigator must determine the normal behavior of the interviewee at the beginning of the interview so that he will recognize behavioral symptom changes.

Also, the investigator must be able to recognize interviewee defenses and disarm the interviewee’s defensive tactics. Defenses consist of circling, changing to directive

approach; memory loss, asking follow up questions; and offense, diffuse the move by minimizing the situation.

- ***Admission-seeking interview***

The admission-seeking interview is designed to obtain a truthful confession. The three types of admission-seeking interviews are as follows:

- Shock interview – designed to shock the interviewee into a truthful confession
- Pressure interview – designed to elevate the anxiety of the interviewee to a level of truthful confession
- Good buddy interview – a friendly fashion interview designed to convince the interviewee to truthfully confess

- ***SAS 99 interview***

Statement on Auditing Standards 99 requires auditors to inquire of appropriate officials about the possibility of, or their knowledge of, fraudulent activity. The standard provides employees to interview, example questions and describes how to conduct the interviews.

Chapter V

Other Investigative Techniques

Two other techniques employees need to be familiar with are expert and fact witness testimony and written confessions.

- ***Expert and fact witness testimony***

The difference between expert and fact witness testimony is that the investigator as an expert witness may give his expert opinion. A fact witness is limited to testifying only about facts. A judge has to opine that the investigator is considered an expert witness.

A CPA testifying as an expert witness under the PEEC professional standards when asked if he is independent must answer that he is not considered independent under the standard when testifying as an expert witness. As a fact witness the CPA is considered independent.

The expert and fact witness principles and techniques are too voluminous to be discussed for this course.

- ***Written confessions***

The investigator must understand the principles of taking a written confession. The most important principles involve the interviewee initialing each page and signing and dating the statement, and including a statement that, “My statement was given of my own free will.” The interviewer must also sign and date the statement. Other important principles of written confessions are not discussed in this course due to time limitations.

Chapter VI

Evaluating and Investigating Fraud Risks

Evaluating and investigating fraud risks involves a myriad of principles that employees should be taught. They include:

- Knowing what a white-collar criminal looks like
- Recognizing certain fraudster characteristics
- Knowing the employee behavioral changes that indicate a fraudster
- Understanding the fraud triangle elements
- Knowing how a fraudster thinks
- Understanding risk analysis principles relating to internal control deficiencies
- Identifying the occupational fraud schemes associated with internal control deficiencies
- Understanding the concealment methodologies associated with each type of occupational fraud scheme
- Knowing the red flags of occupational fraud
- Knowing the appropriate investigative procedures to execute relative to specific fraud risks, specific occupational fraud schemes and related concealment methodologies, and red flags
- Understanding the follow-up investigative procedures to execute after confirmation of a fraud

- Knowing the appropriate internal controls to recommend to address internal control deficiencies

These principles are too voluminous to discuss in this course.

Chapter VII

Investigator Traits

There are three important traits that successful investigators have. These traits are skepticism, questioning mind, and being extremely attentive to the detail of everything heard or observed during the investigative processes. SAS 99 requires CPAs to exercise professional skepticism and a questioning mind.

My definition of skepticism is different than SAS 99's definition. SAS 99 states that the CPA should not trust nor distrust. I believe the fraud investigator should not accept anything at face value -- trust nothing and question everything. Obviously, the investigator has to match available resources to investigative procedures.

Chapter VIII

Relevant Assertions

Employees need to consider and understand how to apply the relevant assertion test for relevant fraud risks. When assessing the risk of fraud, the investigator should consider the relevant assertions outlined in SAS 106.

SAS 106 states that CPAs, regardless of the assessed risk of material misstatement, have a responsibility to design and perform substantive procedures for all relevant assertions related to each material class of transactions, account balances, and disclosure to obtain sufficient appropriate audit evidence. The SAS 106 definition of relevant assertion is “assertions that significantly impact fair presentation of financial statements.” The relevant assertions are presented below.

- **Account balances**
 1. Rights and ownership
 2. Existence
 3. Valuation and allocation
 4. Completeness

- **Classes of transactions**
 1. Occurrence

2. Accuracy
3. Completeness
4. Cut-off
5. Classification

- **Disclosure**

1. Occurrence, rights and obligations
2. Completeness
3. Classification and understandability
4. Accuracy and valuation

Chapter IX

Investigating Cash Receipts

The first step in investigating fraud is evaluating the risk of fraud. This involves assessing and testing for the elements of COSO (Committee of Sponsoring Organizations). The investigator also conducts SAS 99 interviews and brainstorming. Employee behavioral changes should be determined and evaluated. Internal controls are evaluated for effectiveness. The possibility of management override of controls and collusion should be considered.

The next step is to determine which occupational fraud schemes could be perpetrated based upon the results of the risk analysis. For example, the two choices relating to cash receipts are cash larceny or skimming.

The third step is to develop an investigative audit plan. Standard investigative procedures would include:

1. Trace source documents to receipts to cash journal recordings to deposits;
2. Conduct a surprise cash count;
3. Review bank reconciliations;
4. Confirm bank activity; and
5. Prepare a proof of cash.

The next step is to determine which concealment methodologies should be tested by the investigator.

1. Lapping

2. Check/cash substitution
3. Accounts receivable kiting or lapping
4. Bank account kiting
5. False deposit
6. Improper record creation, alteration or destruction
7. Posting false entries

Then, the investigator has to select the investigative audit procedures to test the various concealment methodologies. The procedures are discussed as part of Chapter X, *Cash Receipt Risk Factors and Red Flags*.

Chapter X

Cash Receipt Risk Factors and Red Flags

This chapter is presented as an example of the risk factors and red flags employees should be trained to detect. The chapter presents 40 risk factors and red flags associated with cash receipts. Cash receipt frauds consist of cash larceny and skimming. The frauds involve a myriad of concealment methodologies, e.g., lapping; check/cash substitution; bank account kiting; false deposit-in-transit scheme; and altered, created, duplicated documents, etc. Cash receipt schemes primarily relate to misappropriation of assets.

- ***Failure to log cash at original point of entry into the organization***

If cash is not logged into an organization at the original point of entry, the risk of skimming is elevated. The fraudster simply steals the funds at the original point of entry into the organization. Detection procedures involve placing cameras over the original points of cash entry, investigation of customer billing complaints, employee interviews, accounts receivable confirmations, and trend analysis.

- ***Lack of restrictive endorsements on customer checks***

This is a risk factor for cash larceny. The lack of restrictive endorsements, e.g., “For Deposit Only ABC Corp.,” being placed on customer checks increases the likelihood of

the check being stolen, the payee being altered, and a false endorsement being used to improperly negotiate the check. Examination of bank microfilm of deposited checks, employee interviews, following vendor payments, and inspection of deposits before being taken to the bank detect this risk factor.

- ***Receipt device alterations***

An alteration of the receipting device, e.g., cash register or computer, is a red flag for cash larceny. The fraudster alters the receipting device to record only a portion of the proper receipt amount on the device. Detection procedures involve comparison of cash receipting device reports to known merchandise pricing, trend and pattern analysis of receipting, monitoring cameras located over receipting devices, and employee interviews.

- ***Cash register recording manipulation***

This cash registering scheme involves the fraudster not recording/under recording sales and stealing the unrecorded revenue. Also, it involves processing inappropriate voids to the cash reports. The fraud scheme is detected by examination of receipt reports, trend and pattern analysis of receipting, camera monitoring, and employee interviews.

- ***Organization receipts deposited to employee's personal bank account***

This red flag is detected by examination of the deposits to an employee's personal bank account. The investigator is looking for stolen organization checks that are deposited into the employee's bank account. The detection procedure is not a routine audit procedure mandated by the Statements on Auditing Standards issued by the Auditing Standard's Board of the American Institute of Certified Public Accountants. It is a routine examination procedure if the investigator determines organization funds have been inappropriately deposited into an employee's personal bank account. The procedure normally involves obtaining a subpoena for the employee's bank records from a prosecuting attorney. If the investigator does not have the authority by law to approach the Prosecuting Attorney directly, e.g., law enforcement agency, etc., the investigator should obtain the permission of those in governance before approaching the Prosecuting Attorney.

- ***Cash count does not match records***

The cash count should always be conducted on a surprise basis. If the count purpose is to test for receipt larceny, the investigator counts receipts from the last deposit and compares the receipts to available cash on hand. If the count's purpose is to test cash fund balances, e.g., petty cash funds, the investigator counts the available cash funds plus the invoices evidencing unreimbursed payments from the fund, and compares total counted funds and disbursement documentation to the recorded balance of the fund. A shortage in either process represents a red flag for cash larceny.

- ***Receipts not deposited***

This is a red flag for cash larceny. Detection procedures include surprise cash counts, comparison of receipts to deposits, employee interviews, trend and pattern receipting analysis, camera receipting area monitoring, and investigation of customer complaints.

- ***Generic handwritten receipts***

The use of generic handwritten receipts has always been a red flag for cash larceny. In today's world, especially with the prevalence of IT business processes, it is even more of a red flag. The fraud risk associated with generic receipts involves the lack of accountability. The receipts do not have the name of the organization; are handwritten, not pre-numbered; and in the case of a fraud, are not recorded in the cash receipt journal. The investigator detects the use of generic receipts by employee inquiry, observation of office business practices and records, examination of written business policies, and by investigating customer complaints. If the investigator determines generic receipts are being issued, the generic receipts should be reconciled to entry into the organization's accounting system. The investigator is examining for generic receipts torn out of the receipt books and discrepancies between the amount of the generic receipts and the recorded official receipt amounts, i.e., skimming. Another investigation procedure involves comparison of known sales/service unit pricing to recorded unit pricing. Discrepancies should be confirmed with payors, e.g., compare known fine for 1st offense DWI, \$500, with individual amounts collected for fines, etc.

- ***Both manual and computer receipts issued for same sales***

The use of both manual and computer receipts elevates the risk of skimming or cash larceny. The fraudster issues manual, pre-numbered receipts containing the name of the organization and then re-enters the receipts into the official IT accounting system at lesser amounts. This fraud scheme is detected by reconciling the manual receipts to electronic receipts deposited.

- ***Receipts do not make sense***

If receipts are illogical, this is a red flag for larceny or skimming. The abnormalities include unknown customers, abnormal collection dates, alterations without explanation or documentation, and abnormal receipt issuers. The abnormal receipts are detected by examination of individual receipts and by payment confirmation with payors.

- ***Receipts are improperly valued***

This is a red flag for skimming. The red flag is detected by trend and pattern analysis and by comparison of known pricing with receipt amounts. The investigation involves monitoring cameras placed over receipting areas and confirmation of customer payments. Often unofficial generic or other unrecorded receipts have been issued to customers in the correct amounts.

- ***Unrecorded receipts issued out of sequence and without authorization***

Unrecorded receipts issued without authorization and out of sequence should be considered red flags for cash larceny and skimming. Fraudsters may issue unrecorded receipts that are not in sequence, nor authorized. This is a variation of the duplicate or generic receipt schemes, except the fraudster issues an official receipt assuming that the lack of recording will not be discovered. In non-IT accounting systems, investigators should examine unused receipt books looking for inappropriately issued receipts located commonly at the back of the unused receipt books. In IT accounting systems, queries of all issued receipts should be executed and reviewed.

- ***Supplemental accounting records do not agree with issued receipts***

This is a red flag for skimming. If original source documents, e.g., licenses, permits or citations, etc., do not support the amount of recorded receipts for these documents, skimming is a probable reason for the differences. Detection involves comparing source revenue documents with receipts issued, employee interviews and receipt trend analysis.

- ***Numerical skips in receipt numbers deposited***

Skips in receipt numbers deposited are red flags for cash larceny. The flags are detected by comparing receipts to deposits and query of all receipt numbers deposited, which facilitates detection of undeposited receipt numbers. Undeposited receipt numbers should

be investigated including confirmation with payors or inspection of supplementary revenue records evidencing receipts.

- ***Duplicate receipts noted***

The discovery of duplicate receipts is a red flag for cash larceny or skimming. The duplicate set of receipts, customarily, will equal the deposits and the cash receipt journal recordings. The original set of receipts equals the authentic amount of customer payments. This fraud scheme is detected by trend and pattern receipting analysis; comparison of known pricing with receipted amounts; recognition of the abnormality of a perfect set of receipts, e.g., no voids or corrections; customer confirmations; employee interviews; monitoring of hidden receipting area cameras; inspection of the receipting office for the original set of receipts, etc. Fraudsters may maintain original and duplicate receipts in their office for convenience of executing the fraud scheme.

Do not open/break into a government employee's locked desk without permission, a subpoena, or an organization policy authorizing access acknowledged in writing by the employee. One state law requires the employee to be on site when locked desks are accessed. After discovery of the duplicate receipts, the investigator should obtain the original receipts for comparison with the recorded duplicate receipts.

- ***Receipt alterations noted***

Unexplained receipt alterations are a red flag for skimming. Alterations can include payor, date, amount and explanation. Payor alterations involve skimming the original payor's payment or accounts receivable lapping. Date alterations are involved in lapping. Amount alterations normally involve skimming all or part of the customer's payment. Explanation alterations involve attempts to support payor, date or amount alterations. This red flag is detected by inspecting receipts.

- ***Receipt voids not documented***

Undocumented voided receipts are a red flag for cash larceny. Legitimate receipts are improperly voided to conceal cash larceny. Detection involves queries and trend analysis of voided receipts, and confirmation of the voided receipts with payors.

- ***Receipt voids not properly approved***

Organizations should have oversight approval controls for voiding receipts. If voided receipts do not contain these proper approvals, this is a red flag for cash larceny. This is detected by examining voided receipts for proper approvals. In IT accounting systems, reports should be generated matching voids with approvals and variances should be investigated.

- ***Unusual amount of receipt voids***

Excessive numbers of receipt voids should be considered a red flag for cash larceny.

Query reports of voids should expose the abnormality. Trend analysis of voids is another investigative tool. Voided receipts should be investigated for legitimacy.

- ***Failure to issue receipts for checks***

This red flag relates to cash larceny and the concealment methodology of check/cash substitution. The fraudster steals receipted cash and substitutes unreceipted checks in deposits identified as being the receipted cash. This fraud scheme is prevalent in business processes lacking cash receipting and handling internal controls where there is a significant amount of cash received, e.g., water systems, municipal courts or police departments, etc. One detection procedure involves comparison of check/cash composition of receipts to deposits. If there are more receipts for cash than cash deposited, this is one of several red flags for check/cash substitution. However, a possible nonfraud explanation could be the cashing of accommodation checks.

Accommodation checks are checks cashed for the convenience of employees and others out of receipted cash on hand.

- ***Check/cash composition of receipts does not equal check/ cash composition of deposit***

This abnormality is a red flag for check/cash substitution. Check/cash substitution is a concealment methodology for cash larceny. Detection involves the reconciliation of the amount of cash receipted to the cash deposited. Also, the amount of checks receipted is compared to the amount of checks deposited. Check/cash substitution is indicated when cash receipted is less than cash deposited and checks receipted are more than checks deposited. This comparison assumes the organization's policy requires depositing intact. The investigator must determine if the organization allows accommodation checks to be cashed.

- ***Receipt names do not match check names deposited***

This is another red flag for check/cash substitution. The flag is discovered by reconciling names on checks deposited to names on receipts. Variances should be investigated by confirming payment information with the payors of checks that are deposited and not unidentifiable to receipts. This process is particularly effective in business environments where receipts are required to be issued in the payor's name. Check deposit information is obtained directly from the organization's bank, e.g., paper documents, electronic banking documents, bank images, bank microfilm, etc.

- ***Unreceipted checks are noted in surprise cash counts***

Surprise cash counts that contain unreceipted checks are red flags for check/cash substitution. Fraudsters sometimes maintain unreceipted checks in the cash till or bank bag until sufficient receipted cash is received to execute check/cash substitution.

Therefore, if unreceipted checks are discovered in surprise cash counts, the investigator should examine for check/cash substitution. Examination procedures include obtaining bank documentation of checks deposited and tracing the checks to receipts.

- ***Checks cashed without use of organization deposit slips***

Fraudsters conducting check skimming must convert the checks to cash. This occurs by the fraudster cashing the checks either directly before or after the bank deposit of the organization's receipts. The fraudster is at the bank making the organization's deposit, and, therefore, cashing the organization's checks is perceived by bank tellers as normal activity. The fraudster does not list the checks on the deposit slip with cash back, because this leaves an audit trail of the cashed checks. Generally, one of two scenarios exist -- either the fraudster is inappropriately cashing unreceipted organization checks or the receipted cashed checks are being hidden by one of the cash larceny concealment methodologies, e.g. lapping, bank account kiting, etc.

- ***Customer checks with questioned endorsements***

Customer checks containing questioned endorsements are red flags for skimming.

Customer canceled checks to be examined should be obtained directly from the customer or bank. Questioned endorsements indicate the check was negotiated outside the organization and would not have been recorded in the organization's accounting system.

This procedure is executed in circumstances when the investigator has suspicions that customer checks have been skimmed and negotiated outside the organization.

- ***Customer checks with unauthorized second endorsements***

Customer checks with second endorsements should be considered a red flag for skimming. Customer complaints about billings not containing credits for payments or complaints about the second endorsement are indicators of this fraud scheme. Customer checks should only contain the endorsement of the organization. Second endorsements indicate the customer's check was negotiated outside the organization. Copies of customer checks containing second endorsements should be followed to deposit.

- ***Customer checks with no endorsements***

If the organization has a policy requiring restrictive endorsements on checks, customer checks with no endorsements are red flags for cash larceny or skimming. The fraudster has a means of negotiating the stolen checks without endorsement, e.g., friend at a bank or who owns a business, fraudster owns a business, etc. Further investigative procedures include obtaining a copy of customer checks and following them to deposit. If a bank

employee is involved, the bank investigative staff should be alerted to the fraud scheme. Most likely, the bank employee is receiving an undisclosed, inappropriate personal benefit for cashing the stolen checks.

- ***Employee's cash count sheets evidencing transfer of funds do not reconcile***

Cash count sheets are used in some organizations to document the transfer of funds from one employee to another. If the amount of receipts on the copy of the transfer sheet maintained by the transferring employee does not equal the cash receipts on the transferred employee's cash count sheet, this is red flag for skimming on the part of the transferred employee.

- ***Only one copy of cash count sheet evidencing transfer of funds is maintained***

The risk of cash larceny or skimming is elevated in organizations that do not require employees to maintain a copy of cash count sheets, which evidence transfer of receipts between two employees. If both employees do not maintain a copy of the cash count sheets evidencing transfer of funds, detection or assignment of responsibility for discrepancies is severely hindered.

- ***Trend receipt analysis reveals unusual relationships***

If receipt trend analysis reveals abnormalities, these are red flags to be further investigated.

Further detection procedures are specific to the abnormality and can involve tracing receipts to cash receipt journal posting to deposits. Examination of supplementary revenue records and confirmation of payments and voids with payors may also be necessary. Following the funds from payor to deposit may be necessary. Other examination procedures may include employee interviews and receipt pattern analysis.

- ***Pattern receipt analysis reveals unusual relationships***

Abnormal receipting patterns noted by monitoring daily receipting activity is a red flag for cash larceny. Examples of abnormal activity could be during one employee's shift:

- Large amounts of returns and related credits
- Consistent cash till shortages
- Unusually low recorded sales
- Unusually low cash sales
- Unreceipted checks routinely discovered in the cash till

After discovery of the flag, a hidden camera should be installed to catch the employee stealing.

- ***Cash receipt edit report anomalies***

Anomalies on cash receipt edit reports are red flags for cash larceny, e.g., receipt data changes that are unreasonable or without explanation or documentation. The receipt edit should be investigated to determine that it was properly approved, legitimate, and documented.

- ***Cash receipt edit reports are not generated or monitored***

If the organization does not generate or monitor receipt edit reports, the organization is at a higher risk of cash larceny. Changes could be made to the receipts that conceal cash larceny and management would never detect the fraud. The reports should be examined for proper edit approvals, documentation, and reasonableness. Questioned edits should be further investigated by confirmation with customers, examining accounts receivable, and employee interviews.

- ***Credit card credits unrelated to purchases***

Clerks may post credit card credits to their own credit card that are unrelated to their personal purchases, which indicate merchandise returns or voided sales. Trend and pattern analysis of receipts should detect this scheme.

- ***Altered customer revenue checks***

This is a red flag for cash larceny or skimming. Indicators of altered customer checks include customer complaints concerning subsequent billings, not providing credit for earlier payments, or alterations on customer canceled checks. If customer canceled checks provide evidence of alteration of organization payments, this anomaly should be further investigated. Further investigation procedures include following the customer payments from the customer to deposit.

- ***Customer checks cashed at the same unauthorized location***

This indicates customer checks are being skimmed and cashed at a location where the fraudster has a relationship with the cashing organization. All customer checks cashed at the unauthorized location should be investigated. Indicators of this fraud are customer complaints concerning customers not receiving credit for payments on subsequent billings and numerous canceled check bank routing and endorsements indicating the checks were cashed at the same abnormal location.

- ***Deposits contain unreceipted cash***

This is a red flag for skimming. Fraudsters sometimes will collect revenue and place it in the till with the intent of stealing the revenue after the day's closing. Fraudsters are less subject to scrutiny after hours. Investigators may confirm skimming by examining records other than receipts evidencing revenue, e.g., contracts, licenses, or permits; by confirming payments with customers; examining customer complaints; monitoring cameras located over cash receipting areas; etc.

- ***Revenue contract variances between minimum revenue due and revenue recorded and deposited***

If significant minimum contract revenue has not been receipted and deposited, this is a red flag for skimming. Significant minimum contract revenue due the organization should be reconciled to contract revenue recorded and deposited. Variances detected in the examination should be further investigated by obtaining documentation of the contractor's payments to the organization. If the contractor has made the payments due, the payments should be followed to deposit, and a determination should be made as to why the payments were not recorded and deposited to the organization's bank account.

- ***Contract manipulations***

Altered office copies of contracts are red flags for concealment of skimming. The fraudster alters the contract to reflect less minimum revenue due then steals the difference between the customer payments and the altered contract amount. This is detected by inspection of contracts, confirmation of the contract with the customer, review of board minutes, and employee interviews. After detection of the red flag, the investigator should obtain copies of the customer's canceled checks and follow them to deposit.

- ***Ending cash balances in amounts less than daily deposits***

This is a red flag for cash larceny. Normally, ending cash balances should not be less than daily deposits. The indication is fraudsters are depositing receipts and then stealing

some of the receipts before day's end. This is detected by a query of deposits and ending bank balances. After detection, the investigator should analyze those accounts for this flag and determine why the bank account balance is always less than daily deposits. Clearing accounts are exceptions to this red flag rule.

Chapter XI

Other Risk Factors and Red Flags

There are over 800 risk factors and red flags related to the following areas for which course time limitations do not permit discussion. State Auditors should train staffs how to detect and properly respond to the risk factors and red flags related to the areas listed below.

1. Records
2. Abnormal Relationships
3. Behavioral Changes
4. Board
5. Internal Controls
6. Complaints
7. Cash
8. Investments
9. Accounts Receivable
10. Inventory
11. Allowances and Reserves
12. Assets
13. Subsidiary Accounts
14. Notes to Financial
15. Sales and Revenue
16. Journal Entries

17. Bank Statements and Reconciliations
18. Budgets
19. Purchasing, False Billing and Disbursements
20. Payroll
21. Employee Reimbursement
22. Check Tampering

Chapter XII

Summary

This course is designed to inform State Auditors of the principles of fraud investigation that should be taught to auditors.

Employees should be taught how to recognize and respond to:

1. Employees demonstrating fraud characteristics
2. Fraud risk factors and
3. Red flags

by utilizing fraud risk analysis and detection tools discussed in this course. Also, employees should be taught how to conduct professional interviews, SAS 99 interviews and admission-seeking interviews. The employees need to know the principles of providing expert-witness and fact witness testimony. They also have to know how to take a written confession so that it will pass court challenges. Employees need to be taught how to think like a fraudster and the proper methodology for investigating white-collar crime. They also need to be taught the importance of and how to apply the SAS 106 relevant assertions to investigations. This course discusses 40 of the over 800 risk factors and red flags of occupational fraud. Employees need to be taught to

recognize and respond to all 800 plus risk factors and red flags. If State Auditors teach employees these fraud investigation principles, the employees will be better equipped, to detect and deter fraud as a routine part of performing audits.

Bibliography

- Allen, Catherine, CPA. “*Auditing Internal Control Over Financial Reporting.*” Lewisville, TX: American Institute of Certified Public Accountants, 2007.
- Alobrecht, W. Steve, Keith R. Howe, and Marshall B. Romney. *Detering Fraud: The Internal Auditor’s Perspective.* Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1984.
- American Institute of Certified Public Accountants, Inc. *Accounting Standards, Original Pronouncements.* “Consideration of Fraud in a Financial Statement Audit,” SAS No. 99, 2002.
- Association of Certified Fraud Examiners, The. *Fraud Examiners’ Manual.* Revised 8th ed. ACFE, 2008.
- Bintliff, Russell L. *White Collar Crime Detection and Prevention.* Englewood Cliffs, NJ: Prentice Hall, 1993.
- Blount, Ernest C. *Occupational Crime: Deterrence, Investigation, and Reporting in Compliance with Federal Guidelines.* Boca Raton, Florida: CRC Press, 2003.
- Blount, Ernest C. *Occupational Crime: Deterrence, Investigation, and Reporting in Compliance with Federal Guidelines.* Boca Raton, Florida: CRC Press, 2003.
- Bologna, Jack. *Corporate Fraud: The Basics of Prevention and Detection.* Boston, MA: Butterworth-Heinemann.
- Bologna, Jack, and Robert J. Lindquist. *Fraud Auditing and Forensic Accounting.* New York, NY: John Wiley & Sons, 1987.
- Bologna, Jack. *Handbook on Corporate Fraud.* Boston, MA: Butterworth-Heinemann, 1993.
- Coderre, David G. *Fraud Detection: Using Data Analysis Techniques to Detect Fraud.* Vancouver: Global Audit Publications, 1999.
- Connelley, Michael, CFE, CPA. “*Auditing for Internal Fraud.*” Lewisville, TX: American Institute of Certified Public Accountants, 2007.
- Dean, Bruce A. “*Wrap It Up: Packing Your Case for Prosecution.*” The White Paper. Vol. 16, No. 1. January/February.

- Dennis, Lynda, PhD, CPA, CGFO. “*Fraud in the Governmental and Not-for-Profit Environments: What a Steal!*” Lewisville, TX: American Institute of Certified Public Accountants, 2007.
- Dennis, Lynda, PhD, CPA, CGFO. “*Frequent Frauds Found in Governments and Not-for-Profits.*” Lewisville, TX: American Institute of Certified Public Accountants, 2007.
- Hall, John, CPA. “*Forensics and Financial Fraud: Real World Issues and Answers.*” Lewisville, TX: American Institute of Certified Public Accountants, 2007.
- Helms, Glenn, CPA, PhD, CISA, CIA. “*Internal Control Essentials for Financial Managers, Accountants, and Auditors.*” Lewisville, TX: American Institute of Certified Public Accountants, 2007.
- Ketz, J. Edward. *Hidden Financial Risk: Understanding Off-Balance Sheet Accounting.* Hoboken, NJ: John Wiley & Sons, Inc., 2003.
- Ramos, Michael J. *Consideration of Fraud in a Financial Statement Audit: The Auditor’s Responsibility Under New SAS No. 82.* New York, NY: The American Institute of Certified Public Accountants, Inc., 1997.
- Snyder, Neil H., O. Whitfield, William J. Kehoe, James T. McIntyre, Jr., and Karen E. Blair. *Reducing Employee Theft: A Guide to Financial and Organizational Controls.* New York, NY: Quorum Books, 1991.
- Wells, Joseph T., CFE, CPA. *Corporate Fraud Handbook: Prevention and Detection.* Hoboken, NJ: John Wiley & Sons, 2004.
- Wells, Joseph T., CFE, CPA. *Occupational Fraud and Abuse.* Austin, TX: Obsidian Publishing Company, Inc., 1997.
- Wells, Joseph T., CFE, CPA. “*Why Employees Commit Fraud.*” *Journal of Accountancy.* New York, NY: The American Institute of Certified Public Accountants, Inc. February, 2001.