ACCA annual meeting 2002

509 Vampires of the Bottom Line: A Look at Corporate Fraud

James J. Eisenhower
Partner
Ballard Spahr Andrews & Ingersoll, LLP

Howard Silverstone
Principal
Kroll Inc.

James A. Stavros, CPA
Principal
Kroll Inc.

Faculty Biographies

James J. Eisenhower

James J. Eisenhower is a partner in the litigation department and a member of the Government Enforcement/White Collar Crime Group of Ballard Spahr Andrews & Ingersoll, LLP.

Mr. Eisenhower was formerly a trial attorney for the U.S. Department of Justice, as well as an assistant U.S. attorney for the Eastern District of Pennsylvania. He has served as special counsel to the Pittsburgh and Philadelphia Housing Authorities, assisting in Inspector General matters and compliance programs. He has also served as chief counsel to the City of Philadelphia's Police Advisory Commission.

Mr. Eisenhower was the Democratic candidate for Pennsylvania State Attorney General in 2000 and served as a delegate to the 2000 Democratic National Convention. He was named by former President Bill Clinton to the 31st class of White House Fellows and served in the Clinton administration as an aide to National Security Advisor Anthony Lake. While at the White House, Mr. Eisenhower was a member of the U.S. Delegation to the Paris Plenary Session of the Financial Action Task Force and a member of the U.S. Delegation at the G-7 Ministerial Meeting on Terrorism. Mr. Eisenhower has been a member of Philadelphia Mayor John Street's Task Force on Police Discipline.

Mr. Eisenhower is a received a BA from Temple University, a JD from Antioch University, and a masters of philosophy from Oxford University, attending as a Marshall Scholar.

Howard Silverstone

Howard M. Silverstone is a principal in the Philadelphia office of Kroll Inc. His responsibilities include project planning and management in a variety of forensic accounting assignments. His work further includes assistance with interrogatories and depositions and assistance at trial. His practice comprises the management of forensic accounting assignments including white-collar crime, complex commercial litigation, insurance claims, and financial due diligence. He has also testified in the Court of Common Pleas in Philadelphia, in Federal Court, in Arbitration, and at depositions.

With over 20 years experience in accounting, Mr. Silverstone has concentrated on forensic and investigative accounting for over 15 years. Prior to cofounding the Philadelphia office of Kroll nearly 10 years ago, he was a director in a forensic accounting firm and worked for five years at an international accounting firm as both a financial investigator and auditor. Prior to that, he was with a public accounting firm in the United Kingdom.

Mr. Silverstone is currently president of the British-American Business Council's Philadelphia chapter. He is a licensed certified public accountant in Pennsylvania as well as a chartered accountant (UK) and a certified fraud examiner.

Mr. Silverstone received his BA with honors from the London Guildhall University, (formerly known as City of London Polytechnic).

James A. Stavros

James A. Stavros, CPA is a principal in the Philadelphia office of Kroll Inc. His practice involves a variety of forensic accounting and investigative assignments, including employee fraud, unraveling complex financial transactions, business interruption, property claims, lost profits/economic damages, personal injury/wrongful death, and financial due diligence. Engaged as a consultant or expert witness, Mr. Stavros provides assistance with interrogatories, depositions, and testimony at trial, if necessary. Mr. Stavros has concentrated on forensic and investigative accounting for nearly 15 years.

Prior to cofounding the Philadelphia office of Kroll, he was a senior associate in a forensic accounting firm and worked for five years at an international accounting firm as forensic accountant. Prior to this, he was a branch manager and lending officer for a large Philadelphia Region Commercial Bank.

Mr. Stavros is member of the American and Pennsylvania Institutes of Public Accountants, a member of the PICPA Philadelphia Chapter Forensic and Litigation Committee, and is a member of the National Association of Forensic Economists.

Mr. Stavros received a BS from Widener University and an MBA from Rider College.

CORPORATE FRAUD - VAMPIRES OF THE BOTTOM LINE - WHO COMMITS FRAUD & WHY

Prepared by:
Howard Silverstone and James Stavros
Kroll Lindquist Avey
8 Penn Center – 16th Floor
Philadelphia, PA 19103

CORPORATE FRAUD - VAMPIRES OF THE BOTTOM LINE - WHO COMMITS FRAUD & WHY

Presentation Notes

1. OPENING REMARKS

If fraud takes root where the ground is fertile, then we must live in an era of especially rich soil: it's estimated that fraud costs the North American economy more than $400 billion a year. But the cost of fraud is much more than just the amount of money that might have been misappropriated:

- companies that are victims of fraud bear the cost of investigating the fraud, of clearing up the problem and of ensuring that there's no recurrence.
- losses due to fraud may lead to layoffs, plant closures or even business failures.
- companies defrauded of funds may miss business opportunities. The misappropriated capital could have been used to create employment, build new facilities or develop better products and services.
- fraud also extracts a huge personal cost. It can have a traumatic effect on individuals, leading, in some case, to marriage breakups, nervous disorders and even suicide.

No one is immune to fraud. A business, agency or individual that thinks it's invulnerable to fraud is, in fact, the most inviting to fraudsters. Too often complacency is the fraudster's best ally. Conversely, the fraudster's toughest foe is a potential target that turns out to be both vigilant and well prepared to meet this challenge.

Fraud does not occur randomly throughout an organization or in statistical proportions. There are areas of any business which are more vulnerable than others. The work environment is the key factor affecting the occurrence of fraud. Fraud, by its very nature usually means that the activities are not easily uncovered or identified. In fact the majority of fraud is found out by accident or misadventure.

We like to tell the story of the senior executive who, over the years had managed to build up a seven-figure bank balance in his Swiss bank account - at his employer's expense. No one knew anything about the situation until the executive was experiencing marital difficulties. At a social function, the disgruntled spouse told another executive's spouse that if she and her husband split up she wanted half the Swiss account. The investigation started shortly thereafter.

The anonymous letter, whether from a loyal employee or vindictive ex-employee, is still an important key to the discovery of fraudulent activity. In some cases the fraud and its cover-up becomes so complicated that the perpetrator will just throw up his/her hands and confess.

The **objective of this presentation** is to provide you with some insight into the human element as it relates to the occurrence of fraud; to recognize red flags or indicators of fraud; and matters to consider when reacting to fraud. Fraud is a study in human behavior. Accordingly we will be discussing:

- The human Element;
- Typical profile characteristics of fraudsters;
- Environmental factors which contribute to the occurrence of fraud;
- Practical Red flags or indicators of fraud;
- Factors which deter fraud; and
- Reacting to the discovery of fraud, among other related topics.

We will also discuss some case examples along the way to illustrate how environmental factors affect the occurrence of fraud and that indicators of fraud are often ignored by those who have not yet developed the mindset that fraud does exist.

2. WHAT IS FRAUD?

Definition of Fraud - Before we discuss Who Commits Fraud and Why we should have a basic understanding of the definition of fraud as well as the types of fraud which are committed on business. The key elements of the definition of fraud are dishonesty and deprivation. Dictionaries, however, have a number of definitions. We have included Black's Law Dictionary definition in our graphic materials attached.

Different Forms of Dishonesty include:

- **Active** - a false story/altered books & records/direct theft of assets
- **Passive** - non-disclosure of key information/material omission resulting in higher management bonus
- The victim of a fraud does not necessarily have to suffer an actual loss to have been defrauded - just exposed to the risk of loss such as being granted security interest in a 3rd mortgage vs. a 1st mortgage.

Let's discuss the **Principal Types of Fraud** in the terminology found in the related federal statutes.

Fraud Statutes - Under the U.S. federal system the prosecution of most common-law white-collar crimes such as embezzlement, larceny and false pretenses, is left to the States. The U.S. laws are often used to prosecute the larger and more serious crimes, primarily, because of the superior resources of federal law enforcement agencies and their nationwide jurisdiction. While the discussion of the law and criminal prosecution of financial crimes is beyond the scope of this presentation we have set out those key statutes which are used to prosecute fraud. However, the current risk of financial statement fraud cases has caused the States and Federal Government to establish new laws and oversight with respect to fraud.

Victims of Fraud primarily comprise businesses and the public, however, this seminar will focus on business as a victim and specifically on discussions surrounding the human element as it relates to management and employees who commits frauds. This presentation will not cover specific elements and the technical mechanics of financial statement fraud, although many of the factors discussed in this presentation are pertinent to this issue.

3. WHO COMMITS FRAUD & WHY?

Who Does It? - Fraud is carried out by people. While computers and other electronic wizardry may be used as the means by which it is done and used to cover ones tracks, it is still the result of human input and motivation.

Human Element - A discussion about the human element is crucial to an understanding of fraud and will assist in the prevention and detection process.

- 20/20/60 Rule of Thumb: It is generally accepted within fraud prevention circles that about 20% of people are inherently honest. Another 20% are dishonest and little will deter them. The remaining 60% may commit acts of dishonesty if the need and opportunity co-exist. This means that up to 80% of the workforce is potentially dishonest depending on the circumstances. The circumstances, of course, will be affected to the degree there are adequate internal controls and they are enforced.
- We don't believe that the honesty of employees is pre-determined based on a statistical relationship. The WORK ENVIRONMENT will set the numbers.
- Thus an honest person with a high degree of personal integrity may commit fraud given a set of situational pressures and high opportunity. Conversely, a person of low personal integrity may NOT commit fraud if he is not exposed

to situational pressures and there are strong controls, which provide little or no opportunity for fraud.

- Management can control the "situational pressures" and the "personal integrity" of employees by knowing their people. Management can control the "opportunities for fraud" through internal controls, good management, good policies and good procedures.

Typical Profile - In our experiences we have identified that there are typical characteristics of a fraudster, however, it must be emphasized that many honest people share the same traits:

- long term employee suggests the person knows how the company and its systems operates
- position of trust means they have signing or procurement authority
- Works overtime often unnecessarily/ Never takes vacation so that the scam is not detected while they are away.

Sounds like people we all know work with – doesn't it? There are also many hidden traits common to fraudsters. You are not expected to know the hidden traits, as they are difficult to identify. How do we then become attuned to them? Trust your instincts; listen to the grapevine. If one person expresses concern it may be sour grapes; however, if you hear the same thing from 10 people then there may be some substance to the concerns. Don't ignore the warnings.

GONE Theory - Often, the acronym GONE is used to explain why fraud occurs.

- **Greed** - is self explanatory
- **Opportunity** - exists when the person works in an environment vulnerable to fraudulent activity such as unenforced or no internal controls, management override, no code of ethics.

- **Need** - usually financial and related to addictive behavior such as drugs, alcohol or gambling. Other times it arises from a desire to maintain an appearance of success or to increase their community profile.

- **Expectation** - suggests the company has non-existent, weak or unenforced controls. Employees know the internal systems and how they can be circumvented.

Environmental Factors - Under the GONE theory "Opportunity" exists when the person works in an environment vulnerable to fraudulent activity. Lets look at some of the environmental factors which may increase vulnerability to fraud:

- trust vs. segregation of duties;
- management domination - issue checks with no support;
- no code of ethics or conflict of interest policy;
- accounting practices - credit memos; write-off of accounts receivable; inventory adjustments; and
- management example - treats suppliers unfairly; boss submits personal expenses as business - employees pick up on it.

Rationalizations - Sometimes fraud is committed for reasons other than those covered under the GONE Theory. For example. fraudsters often convince themselves that they are not actually doing anything wrong. This is reflected in their language.

To illustrate further, let us imagine a man who is a pillar of the community, a respected, honest employee, a man with a background no more criminal than that of most of us. This man finds himself with an unshareable problem and an opportunity to steal money from his company. The chances are very good that if in that situation I walked up to him and said, "Fred, steal the money from your boss", he would look at me in horror as if I had suggested he could solve his problem by sticking a pistol into the face of the local liquor store owner. "Fred, steal the money from your company" probably would bring about less of a horror reaction. Still, honest and trusted persons just don't do those things. However, honest and trusted persons do "borrow", and if I were to suggest that Fred secretly "borrow" some money from his firm, I would have helped him over a tremendous hurdle. Then he can tell himself that he is borrowing the money and can continue to believe that he is an honest citizen, even as he is stealing the boss blind.

There are other reasons why otherwise honest people steal and they include:

Increased Community Profile - increased status, donations to charity, etc.;

Corporate Profile (Power) - climb the ladder through deceit; and

Rainbow Syndrome - where an honest businessman facing a financial crisis may undertake activities that he normally wouldn't do in order to keep his business afloat. He may not remit tax withholdings, inflate accounts receivable to obtain increased bank financing, cheat customers and suppliers - all in the hope that things will turn around and get better.

4. INDICATORS or RED FLAGS OF FRAUD

We have discussed the human element and everyone likely has a fraud awareness mindset as evidenced by the attendance at this seminar. Lets then discuss the red flags, which, when recognized, may assist in the detection of Fraud.

What is a red Flag? It is simply a matter of training your mind to see both the donut and the hole. Too much, too little, too many. For example, identifying a senior officer of a company performing clerical functions or functions outside his job description such as:

- approving certain supplier invoices
- hand delivering checks to suppliers

- taking petty cash to pay casual labor
- signing for the receipt of goods

5. DETERRENTS TO FRAUD

It is always easier to take steps to prevent fraud than it is to detect, investigate and prosecute fraud. In our experience, like the homeowner who installs a security system after he has been burglarized, many corporate loss prevention controls are usually preceded by extensive losses. Our next topic discusses those controls, which act as a deterrent to fraud.

Psychological Deterrents

These are procedures, which communicate and reinforce the expected behavior to management and the employees.

- Creating an atmosphere to discuss problems is an extension of knowing your people. Talking to employees about fraud is like talking to your kids about sex and drugs. It is uncomfortable for both parties and many avoid addressing the issue, as they don't think it can happen to their family. However, fraud does exist and management must acknowledge that it exists.

Fraud Policy

A significant tool that is being increasingly employed by business is the development of a Fraud Policy. The key benefit of having a fraud policy is the strong message it sends - not only to employees, but customers and suppliers as well. Employees, customers and suppliers take comfort in dealing with an organization that encourages an ethical environment. Consider having a toll free fraud hotline number to report activities.

System Deterrents

Train employees on policies & procedures; follow up on dishonest acts.

Physical Deterrents

Security codes, card access to floors, password controls, create physical roadblocks to easy access.

6.1 REACTING TO FRAUD

Now that we have a better understanding of the human element and the indicators of fraud lets discuss what to consider when reacting to fraud. Initial reactions include shock, anger, denial and confusion as to what to do next. Some companies act prematurely by lashing out and terminating the suspected fraudster, which could result in a wrongful dismissal action. Others adopt a wait and see position, which usually results in continuing losses or the potential for evidence to be destroyed. Neither of these strategies work. Firstly you take steps to stop the activity and secure the relevant documentation in consultation with corporate counsel. It’s very important to get counsel involved early to preserve the rights of the company and individual. Without getting into the investigation aspects, the objective of the firm will dictate your response. The objective of the company could range from "Recovery of the Assets" to "enforcing company policy". Fraud may be prosecuted criminally or civilly, or both, in sequence or simultaneously. Burden of proof - beyond reasonable doubt vs. preponderance of evidence.

7. AUDITORS RESPONSIBILITY FOR DETECTING FRAUD

Fraud detection is not the primary objective of a financial statement audit. However, the auditors’ responsibility for detecting fraud is an increasingly controversial area. This is due, in part, to the **Expectation Gap**. The average person's exposure to an accountant/auditor and what they do is usually limited to the tax season or when their taxes are audited. Accordingly, the general public, regardless of the efforts by the AICPA and other professional groups, still lacks a true perception of the role of the auditor. This issue is being thoroughly examined in light of the headline making stories of financial statement fraud and audit failures.

The purpose of this section is to alert you to the reality of fraud and make you aware that, at least in the traditional role, compliance with prescribed standards may not be enough. Fraudsters are out there waiting to prey on the unwary, negligent, naive or willfully blind accountant. The auditor who has a heightened sense of fraud awareness and is attuned to seeing the donut as well as the hole has an advantage when fraud does exist and the red flags are evident. Auditors should be fully aware of their responsibilities under SAS 82 which requires the audit to specifically test for fraud and its material impact on the financial statements.

Why Auditors Fail to Detect Fraud

The public may expect the auditor to detect both massive and smaller frauds. However, the auditor is not given the time, the budget or the scope to detect smaller scale fraud, yet is readily blamed when a small comes to light. Why didn't the auditors catch it? - is a frequent question that is can be the subject of litigation. We have already discussed the various environmental factors, which act as indicators that a higher probability of fraud exists.

8. CLOSING REMARKS

We cannot leave you with a special recipe, a comprehensive checklist or manual on detecting fraud. Although, contained in separate tabs are several “lists of seven” signs of corporate and management fraud, characteristics of fraud prone organizations, situations when fraud is likely to occur, invitations to corporate fraud and corporate environmental red flags. These lists can help you focus on the risk factors in your own company and develop policies, address issues and acknowledge factors in an attempt to contravene or neutralize these risks.

First, however, management must:

- accept that fraud exists and could occur;
- acknowledge the importance of fraud awareness;
- deal with the human factors by hiring honest people and keeping them honest via deterrents to fraud; and
- deal with the environmental factors by adequate and enforced controls, policies and procedures including following-up on all dishonest acts.

As corporate counsel and a senior officer of the company, protecting your bottom line from fraud is a challenging goal. But it can be achieved through the implementation of an effective prevention and detection strategy. What are the elements of such a strategy?

- Understand why fraud is committed;
- Ensuring that factors that may motivate employees to commit fraud are minimized;
- Understanding the opportunities for fraud in the business;
- Pinpointing the exposures and high risk areas and reducing the opportunities for fraud;
- Communicate expected behavior to employees;
- Respond appropriately to identified problems and seek out appropriate sanctions against the perpetrators.

FRAUD IN AN INVESTIGATIVE CONTEXT

Prepared by:
James Eisenhower
Ballard Spahr Andrews & Ingersoll, LLP
1735 Market Street, 51st Floor
Philadelphia, PA 19103

A. SAMPLE GUIDELINES FOR GOVERNMENT INTERVIEWS OF EMPLOYEES

Frequently, government agents seek to interview a company's employees early in an investigation and before counsel becomes involved. Often these interviews are conducted by unannounced visits at employees' homes. The following are some guidelines which Company counsel may use to advise employees of their rights and responsibilities in advance of such contacts:

I. Interviews Are Voluntary

The decision whether or not to be interviewed by the government is yours alone. You have the right to refuse to speak to a law enforcement agent or other criminal investigator if you so choose. Likewise, do not instruct another employee either to answer or not to answer questions from law enforcement agents.

II. Legal Counsel Is Your Right

You have the right to confer with a lawyer before being interviewed and have a lawyer present during an interview. You also have the right to postpone an interview to confer with a lawyer. The right to legal counsel applies to everyone, even if you are only being interviewed as a witness or for general information.

III. Legal Counsel Can Help and Is Available

The company recommends that you talk to a lawyer before making a decision about speaking with a law enforcement agent or criminal investigator. A lawyer will help ensure that you understand your rights and make an informed decision, that proper procedures are followed, and that you are treated fairly. If you decide to be interviewed, a lawyer will also arrange to have the interview at a time you choose and that is convenient for you. The company can provide you legal assistance through a company attorney or arrange for other counsel to assist you. The company may be permitted to pay for your counsel under applicable law.

IV. Government Conduct

It is possible that government representatives could try to discourage someone from exercising their rights or even threaten them for doing so. Such conduct is improper.

V. Always Answer Truthfully

If you decide to be interviewed, with or without counsel, any answers you provide must be truthful and complete. Do not guess, speculate or try to "fill in the gaps" about matters that you do not personally know to be facts. You also have rights in connection with the interview. For example, you have the right to choose the time and place of the interview, and to stop the interview at any time.

VI. Notify the Company

You should notify your supervisor immediately of any government contact, including a request for an interview by a law enforcement agent.

B. SAMPLE GUIDELINES FOR EMPLOYEES DEALING WITH SEARCH WARRANTS AND SUBPOENAS

The following are some guidelines which Company counsel may use in advising employees on what to do if served with a search warrant or subpoena:

SEARCH WARRANTS

I. Verify the Agents' Identity and Get a Copy of the Search Warrant; Do Not Obstruct the Search

Never attempt to stop the agents from entering or interfere with the search. However, you have the right to examine the agents' credentials, and the agents are required to produce a copy of the search warrant. Therefore, ask to see the agents' credentials and record their names and other identifying information and for a copy of the search warrant.

II. Call the Counsel Immediately

If government agents appear at your facility with a search warrant, contact counsel [or other designated person] immediately. Ask the agent to wait for counsel to arrive before commencing the search. If they refuse to do so, however, do nothing to prevent or interfere with the search.

III. Do Not Consent to the Search

Do not make any statement that indicates you consent to or approve the search. If an agent asks for your consent, inform the agent that you are not authorized to consent to the search and that the agents should direct their questions to counsel.

IV. Monitor the Search of Your Work Area

Make notes of anything taken by the agents and any comments that they make. The agents are authorized to search only the areas specified in the warrant and to seize only the items listed in the warrant. If you believe an agent is exceeding the scope of the search authorized by the search warrant, inform the agent, object and notify counsel. Similarly, if you believe the agent is taking material that involves the work product of, or communications with, your own or company counsel, notify the agents of this fact and that the documents should not be reviewed by them. Immediately notify counsel and make a record of any potentially legal related documents taken by the agents. Again, however, make no attempt to interfere with or impede the search.

V. Request Copies of Essential Documents

If documents are seized that may be necessary to continue company operations, notify both the agent and counsel so that a request can be made for copies prior to removal of the documents from the company's premises.

VI. Interviews Are Not Authorized

If an agent asks you during a search to identify the location of specific documents or things, you may identify those locations. However, a search warrant does not authorize agents to interview employees about their work or company business. During the execution of a search warrant, interviews are voluntary, just as they are at other times. You have the right to refuse to answer any questions of government agents. You have the right to confer with counsel. It is your decision.

VII. Obtain an Inventory

At the end of the search, the agents are required to provide an inventory of what they have seized. If counsel has not arrived by the conclusion of the search, be sure to obtain a copy of the inventory from the agents.

GRAND JURY SUBPOENAS

Grand jury subpoenas compel companies or individuals to produce records or testify at a designated date and time, at the location where the grand jury meets. Grand jury subpoenas do not authorize agents to conduct a search or interviews. If you are presented with a grand jury subpoena for company records or things (and there is no search warrant), do not allow a search of company personnel. Instead, call counsel immediately. If you receive a grand jury subpoena to testify, you have the right to confer with a lawyer beforehand, and the company can provide you legal assistance through a company attorney or other counsel.

C. MOTIONS TO QUASH GRAND JURY SUBPOENAS

Motions to quash federal grand jury subpoenas are seldom granted and should be used sparingly. Most issues as to scope, privilege and timing can be worked out with prosecutors informally. It is the rare case where the low probability of winning a motion to quash outweighs the risks inherent in antagonizing a prosecutor who may still have an open mind and who otherwise might not be inclined to invest a lot of time in the investigation.

With that caution, the investigatory powers of a grand jury are not unlimited. "Grand juries are not licensed to engage in arbitrary fishing expeditions, nor may they select targets of investigation out of malice or an intent to harass." United States v. R. Enterprises, Inc., 498 U.S. 292, 299 (1991). Furthermore, although issued in the name of the district court, grand jury subpoenas are issued pro forma without prior court approval. In Re Grand Jury Matters, 751 F.2d 13, 16 (1st Cir. 1984). As such, it is recognized that "these subpoenas are 'in fact almost universally instrumentalities of the United States Attorney's office . . . '" Id. (quoting In Re Grand Jury Proceedings (Schofield), 486 F.2d 85, 90 (3rd Cir.) cert. denied, 421 U.S. 1015 (1975).

Thus, a district court retains the power to quash a grand jury subpoena. In Re Grand Jury Subpoena, 175 F.3d 332, 339 (4th Cir. 1999). This power is embodied in Rule 17(c) of the Federal Rules of Criminal Procedure, which provides that "[t]he court on motion made promptly may quash or modify the subpoena if compliance would be unreasonable or oppressive."

One of the grounds on which a grand jury subpoena may be found unreasonable or oppressive is the irrelevance of the information sought to the grand jury's investigation. This test was set forth in United States v. R. Enterprises, 498 U.S. 292 (1991): "[W]here, as here, a subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the subject of the Grand Jury's investigation." Id. at 301; see also In re Grand Jury Subpoena, 175 F.3d 332 (4th Cir. 1999) (affirming district court's order quashing grand jury subpoena that sought documents that were irrelevant to the investigation); In re Grand Jury Subpoena Duces Tecum, 846 F. Supp. 11 (S.D.N.Y. 1994) (quashing grand jury subpoena and noting that subpoena requested documents that were irrelevant to the investigation).

A grand jury subpoena may also be found to be "unreasonable or oppressive" under Fed.R.Crim. P. 17(c) where it is designed to harass the recipient, or issued for some other improper purpose. See e.g. In re Grand Jury Subpoena, 175 F.3d 332, 340 (4th Cir. 1999) (improper purpose); Kiefaber v. United States, 774 F.2d 969, 974-75 (9th Cir. 1985), opinion vacated and appeal dismissed as moot, 823 F. 2d 383 (9th Cir. 1987) (pattern of government misconduct); In re Grand Jury Matters, 751 F.2d 13, 18 (designed to harass); United States v. American Honda Motor Co., 273 F.Supp. 810, 819 (N.D. Ill. 1967) (same).

A grand jury subpoena may be quashed if it seeks confidential or sensitive material. See e.g., United States v. R. Enterprises, Inc., 498 U.S., 292, 305 (J. Stevens, concurring) (district court may properly consider factors that include whether "the subpoena would . . . call for the disclosure of trade secrets or other confidential information,"); In re Grand Jury, 111 F.3d 1066, 1078-79 (3d Cir. 1997) (quashing grand jury subpoena seeking tapes made pursuant to an illegal privately executed wiretap). Overly broad grand jury subpoenas are also subject to being quashed. See e.g. United States v. Wencke, 604 F.2d 607, 611 (9th Cir. 1979) (quashing overly broad grand jury subpoena); In re Grand Jury Subpoena Duces Tecum, 31 F. Supp. 2d. 542 (N.D.W.Va. 1998) (quashing overly broad grand jury subpoena).

In the Third Circuit, where a witness has challenged a grand jury subpoena, the government is required to submit a "Schofield affidavit." In the affidavit, the government must make a preliminary showing that the information sought by the subpoena is relevant to the grand jury's investigation and not sought primarily for some other purpose. In re Grand Jury Proceedings, 486 F.2d 85, 93 (3d Cir.), cert. denied, 421 U.S. 1015 (1975) (Schofield I); In re Grand Jury Proceedings, 507 F.2d 963, 966 (3d Cir.), cert. denied, 421 U.S. 1015 (1975) (Schofield II). Schofield affidavits may, in appropriate circumstances, be submitted to the district court by the government ex parte. See In re Grand Jury Subpoenas, 223 F.3d 213, 219 (3d Cir. 2000). Upon receipt of the affidavit, the district court "has broad discretion in determining whether further proceedings or discovery are necessary or warranted after reviewing the Schofield affidavit, including in camera hearings, additional affidavits or a hearing." In re Impounded, 178 F.3d 150, 158-59 (3d Cir. 1999). As a practical matter, the non-ex parte version of the Schofield affidavit provided defense counsel is typically so cryptic as to be of little real value. See id. at 152-153.

VAMPIRES OF THE BOTTOM LINE
Corporate Fraud

Fraud Definition

"An intentional act or statement designed to deprive another of money or property by deceit or deception. It includes all surprise, trick, cunning or dissembling, and any unfair way by which another is cheated."

TYPES OF FRAUD

Principal Types of Fraud
Embezzlement

- ✓ *Theft of cash and property*
- ✓ *Unauthorized use of property*
- ✓ *Lapping schemes*
- ✓ *Fictitious vendors*

Principal Types of Fraud
False Statements and Claims

- ✓ Inflated travel & expense claims
- ✓ False labor charges
- ✓ Failure to meet contract specifications
- ✓ Product substitution

Principal Types of Fraud
Kickbacks

- ✓ Gifts / cash
- ✓ Travel
- ✓ Lavish entertainment
- ✓ "Loans"
- ✓ "Consulting fees"

Principal Types of Fraud
Conflicts of Interest

- ✓ ***Ownership in a supplier***
- ✓ ***Supplier employs spouse (or offers to)***

Principal Types of Fraud
Misappropriation of Assets

- ✓ ***May involve management, employees or third parties***
- ✓ ***May involve false or misleading statements and documents***
- ✓ ***Results in a financial statements not being presented in accordance with GAAP***

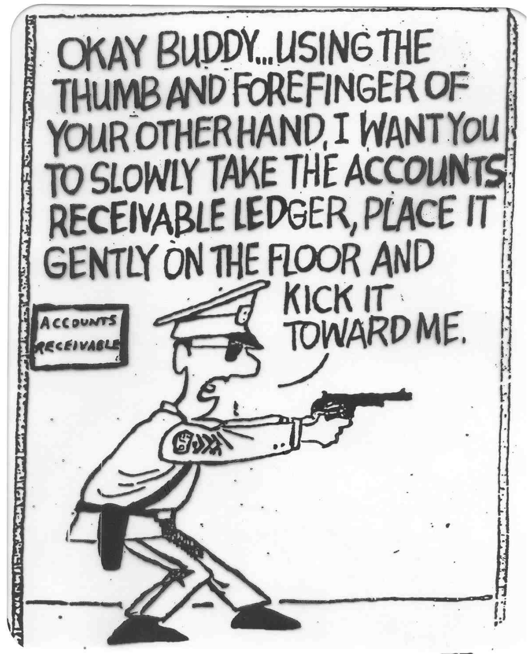
Principal Types of Fraud
Fraudulent Financial Reporting

- ✓ ***USUALLY INVOLVES MANAGEMENT***
- ✓ ***INTENTIONAL MISREPRESENTATION OR OMISSIONS OF SIGNIFICANT INFORMATION ON FINANCIAL STATEMENTS***

The Victims of Fraud

Victims of fraud include:

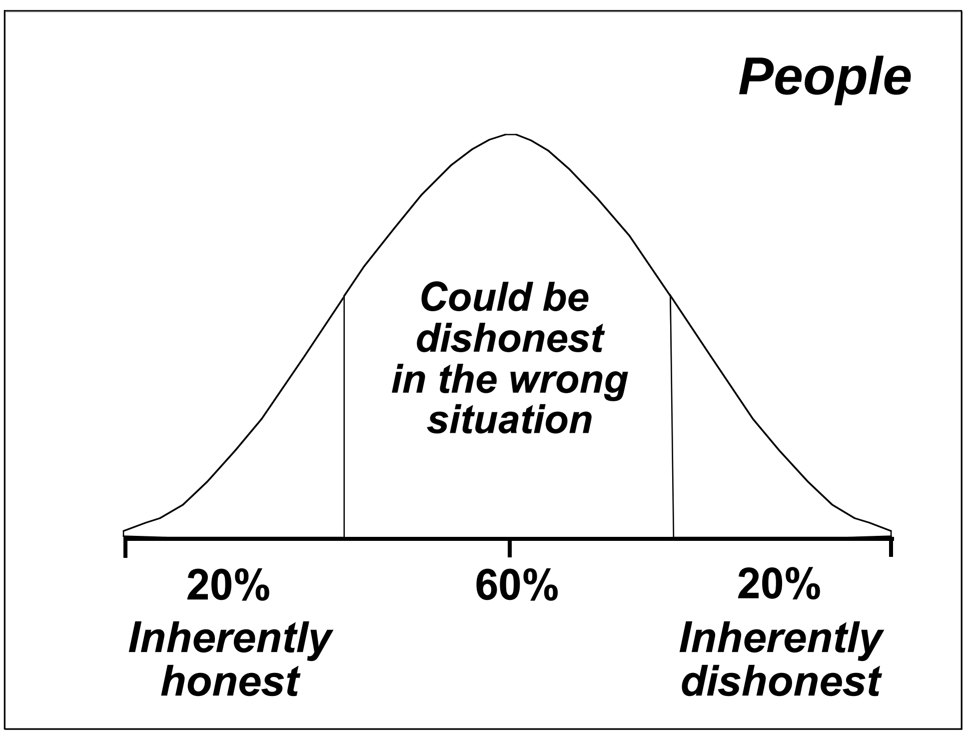
- ✓ ***Business:***
  - ***Internal - employees, management***
  - ***External - suppliers, customers***
- ✓ ***The Public***



WHO COMMITS FRAUD - AND WHY?

Who Commits Fraud?

Suppliers	*False invoicing, short shipment*
Competitors	*Espionage, profit fixing*
Con Men	*False sale of advertising products*
Customers	*Planned bankruptcy, false credit info*
OFFICERS	*FALSE FINANCIAL REPORTING*
Managers	*Kickbacks, expense account fraud*
Other Employees	*Theft of assets, lapping*
Directors	*Manipulate share prices, related party transactions*



Chances of Fraud

MOTIVATION \ OPPORTUNITY	Low	High
Low	Improbable	Possible
High	Possible	Probable

FRAUD

Typical Profile

Outward Traits

- ✓ Long term employee
- ✓ Position of rust
- ✓ Works overtime
- ✓ Never takes vacations

Hidden Traits

- ✓ Living beyond means
- ✓ Emotional instability
- ✓ Drug or alcohol problem
- ✓ Gambler

The GONE Theory

✓ Essential ingredients for a fraud to occur:

✓ G	✓	Greed
✓ O	✓	Opportunity
✓ N	✓	Need
✓ E	✓	Expectation of being caught is low

What Elements Are Usually Present

Pressure:

- ✓ UNREALISTIC EARNINGS TARGETS
- ✓ Pressure to keep up certain lifestyle

Opportunity:

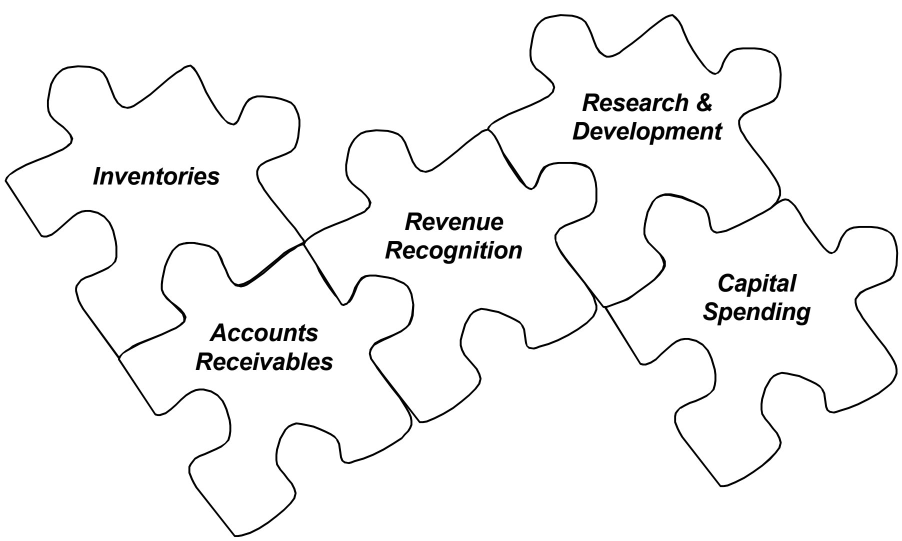
- ✓ Loose internal controls

Managing Earnings

CAN EARNINGS BE MANAGED?

YES ***NO***

Five Ways to Manage Earnings



Typical Factors
Environment Which Fraud Occurs

- ✓ Trust is placed in employees
- ✓ Employees have detailed knowledge of the accounting systems and its weaknesses
- ✓ Management domination subverts normal internal controls
- ✓ Expected moral behavior is not communicated to employees
- ✓ Unduly liberal accounting practices

Typical Factors
Environment Which Fraud Occurs

- ✓ Ineffective or nonexistent internal auditing staff
- ✓ Lack of or ineffective internal controls
- ✓ Poor accounting records
- ✓ Related-party transactions
- ✓ Large unusual transactions
- ✓ Incomplete and out of date procedural documentation
- ✓ Management sets bad example

Typical Factors
Management Characteristics

- ✓ FAILURE TO DISPLAY, COMMUNICATE & SUPPORT APPROPRIATE ATTITUDE REGARDING INTERNAL CONTROL AND FINANCIAL REPORTING
- ✓ High management turnover
- ✓ Domination by an individual or small group

Typical Factors
Management Characteristics

- ✓ Strained relationship with current or predecessor auditors
- ✓ Significant percentage of management's compensation related to the achievement of unduly aggressive operating targets

Typical Factors
Management Characteristics

- ✓ ***NON-FINANCIAL MANAGEMENT'S EXCESSIVE PARTICIPATION IN DETERMINATION OF ESTIMATES OR ACCOUNTING PRINCIPLES***
- ✓ ***Known history of security laws violations***

Typical Factors
Industry Conditions

- ✓ ***Declining industry***
- ✓ ***High degree of market saturation or competition***
- ✓ ***Rapidly changing industry (Technology / rapid product obsolescence)***
- ✓ ***New accounting, statutory or regulatory requirements that could impair the financial stability of the entity***

Typical Factors - Possible Rationalizations

Invariably, fraudsters develop rationalizations for committing fraud. Examples include:

- *"I'm just borrowing the funds."*
- *"I deserve it - I'm underpaid."*
- *"I worked overtime but didn't get paid for it."*
- *"I should have been promoted by now."*
- *"I'm not hurting anyone."*
- *"Everyone else is doing it."*

INDICATORS OF FRAUD - RED FLAGS

Business Red Flags

- ✓ ***Override of normal controls by management-officers***
- ✓ ***Irregular and poorly explained management activities***
- ✓ ***Problems or delays in getting requested information***
- ✓ ***Significant or unusual changes in customers or suppliers***

Business Red Flags

- ✓ ***TRANSACTIONS WHICH LACK DOCUMENTATION OR NORMAL APPROVAL***
- ✓ ***Employees hand delivering checks***
- ✓ ***Customer complaints about delivery and recording of payments***
- ✓ ***Poor computer file access & password change controls***

Business Red Flags

- ✓ Highly complex transactions near year end
- ✓ Overly complex organizational structure
- ✓ Strong pressure to obtain additional capital necessary to remain competitive

Business Red Flags

- ✓ Significant bank accounts in tax-havens for which there is no apparent business justification
- ✓ Inability to generate cash flow
- ✓ Poor or deteriorating financial position

Personal Red Flags

- ✓ *Living beyond means*
- ✓ *Dissatisfied or frustrated with job*
- ✓ *Unusually close association with suppliers*
- ✓ *Severe personal financial losses*
- ✓ *No vacations*

Personal Red Flags

- ✓ *Addiction - drugs / alcohol / gambling*
- ✓ *Change in personal circumstances*
- ✓ *Outside business interests*
- ✓ *Consistently rationalizes poor performance*

DETERRENTS TO FRAUD

Deterrents to Fraud

- ***Psychological***
- ***System***
- ***Physical***

Psychological Deterrents

- *Employee education*
- *Code of ethics*
- *Random or surprise audits*
- *Atmosphere to discuss problems*

System Deterrents

- *Adequate documents and records*
- *Proper procedures for authorization*
- *Supervision and control*
- *Segregation of duties*
- *Employee programs*
- *Hiring practices*
- *Internal Audit*

Physical Deterrents

Combination locks

Card access

24 hour security

Password controls

AUDITOR'S RESPONSIBILITY FOR DETECTING FRAUD

Auditor's Responsibility to Detect Fraud

"The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud."

- SAS No.1, as amended by SAS No.82, AICPA, Professional Standards, vol.1, AU sec.110, par.2

SAS 82

- ✓ ***Describes fraud and its characteristics***
- ✓ ***Requires auditor to assess risk of fraud prior to audit and provides categories of fraud risk factors to consider***
- ✓ ***Provides guidance on how to respond to results of risk assessment***

SAS 82

- ✓ *Identifies two types of fraud the auditor should consider:*
  - ❑ *Misappropriation of assets*
  - ❑ *Fraudulent financial reporting*

Proposed New Statement on Fraud

- ✓ *Discussion of fraud required among audit team members*
- ✓ *Expanded inquiries of management*
- ✓ *Expanded guidance on revenue as a likely risk*
- ✓ *Renewed emphasis on professional skepticism*

What would you do?
The 'Poison Pen Letter'

What would you do?
'Poison Pen Letter'

You have just received an anonymous letter alleging improprieties on the part of one of your employees.

Specifically, the letter accuses one of your construction managers of receiving personal benefits in the form of bribes and work done on his personal residence.

What would you do?
'Poison Pen Letter'

Coincidental with this, your company has just completed the construction of a new facility in Newark, NJ. There were many problems associated with the job including cost overruns of $5 million on a $65 million project.

This project was managed by the same employee against whom allegations of improprieties were made in the anonymous letter.

What would you do?
'Poison Pen Letter'

How would you deal with this situation?

- ✓ ***Do you investigate this matter?***
- ✓ ***If so, who do you assign to the investigation?***
- ✓ ***How do you deal with the construction manager?***
- ✓ ***When do you call in the police?***

Seven Characteristics of Fraud-Prone Organizations

1. Certain management is low-trust, autocratic, focused on profits and economic rewards on a short-term basis, ambivalent about social issues, hostile toward competitors, regulators, customers, stockholders and one another.

2. Financial and operational planning is poor, with persistent cash flow shortages despite an optimistic outlook.

3. Company loyalty is poor, as is employee morale and work motivation.

4. Unusual turnover among non-supervisors, supervisors, middle managers, senior managers, outside auditors and outside counsel.

5. The company or any division is dominated by one manager.

6. The company has a waning line of products or services with little research and development effort.

7. The company is expanding rapidly in a highly competitive and low margin industry.

Seven Situations When Fraud in Books of Account Is Most Likely to Occur

1. Internal controls are absent, weak, or loosely enforced.

2. Company adopts aggressive accounting principles.

3. Employees are poorly managed, exploited, abused or placed under great stress to accomplish unrealistic financial objectives.

4. Certain management models are corrupt, inefficient, or incompetent.

5. A trusted employee has an unresolvable personal problem, of a financial nature, brought on by uncontrolled events.

6. The industry to which the company belongs has a history or tradition of corruption.

7. Unusual turnover in key financial positions.

Seven Invitations to Corporate Fraud

1. Make profit the only corporate objective and the only criteria for performance appraisal.

2. Create a corporate culture in which everyone knows the cost of everything but disregards the value of all else.

3. Create a corporate culture in which profit and economic incentives are the only motivators.

4. Fail to establish an effective code for corporate conduct and a fraud awareness program.

5. Create strong authorization management controls, but do not monitor them for compliance.

6. Ignore complaints from customers, stockholders, employees, and vendors.

7. Fail to monitor management override of internal controls.

Seven Environmental Red Flags of Fraud

1. Do employees have an economic reason to cheat?

2. Does the company suffer from a "we-they" syndrome: management versus non-management personnel?

3. Do conflicts abound among the top management personnel?

4. Is there evidence of spite, hate, hostility, or jealousy among the firm's top management group?

5. Is the history of the firm and the industry regarding regulatory compliance poor?

6. What is the past, present, and future probability of the firm and industry?

7. Are there litigation and complaints pending against the firm by regulatory authorities, vendors, customers, and competitors?

SIGNS OF CORPORATE AND MANAGEMENT FRAUD

1. Changes observed from past behavior pattern of defrauder.

2. Defrauder was undergoing emotional trauma in home or work life.

3. Knowledge that defrauder was a heavy gambler, drinker, had an expensive social life or was sexually promiscuous.

4. Defrauder was heavily in debt.

5. Audit or accounting findings deemed errors or irregularities that were considered immaterial at the time.

6. Knowledge that the company was having financial difficulties such as cash flow shortages, declining sales and/or profits, and loss of market share.

7. Knowledge that management is showing signs of incompetence (i.e. poor planning, organization, controls, motivation, management indecision about corporate mission, goals and management ignorance of conditions in the industry and general economy).

8. Substantial growth beyond the industry norm in regulated industries.

CONSULTING SERVICES PRACTICE AID 97-1

AICPA

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Technical Consulting

Fraud Investigations in Litigation and Dispute Resolution Services

A Nonauthoritative Guide

Ronald L. Durkin
Everett P. Harry III

Management Consulting Services Team

APPENDIX A

SELECTED INDICIA OF FRAUD

The following listing of selected indicia of fraud is presented for illustrative purposes only and is not exhaustive. The conditions listed do not necessarily indicate the existence of fraud; rather, each is an indication that fraud may be present. Many times legitimate activity or other reasons may explain the indicia of fraud. For example, an employee enjoying a lifestyle not readily explained by his or her current earnings may have previously inherited a substantial sum of money. As a result, the CPA should exercise appropriate caution in forming opinions before an adequate investigation. Even then, the CPA should avoid offering opinions about guilt or innocence since the ultimate conclusion of law is a matter for the trier of fact.

Lack of written corporate policies and standard operating procedures

Lack of interest in or compliance with internal control policies, especially division of duties

Disorganized operations in such areas as bookkeeping, purchasing, receiving, and warehousing

Unrecorded transactions or missing records

Bank accounts not reconciled on a timely basis

Continuous out of balance subsidiary ledgers

Continuous unexplained differences between physical inventory counts and perpetual inventory records

Bank checks written to cash in large amounts

Handwritten checks in a computer environment

Continual or unusual fund transfers among company bank accounts

Fund transfers to offshore banks

Transactions not consistent with the entity's business

Deficient screening procedures for new employees

Reluctance by management to report criminal wrongdoing

Unusual transfers of personal assets

Employees living beyond their means

Vacations not taken

Frequent or unusual related-party transactions

Employees in close association with suppliers

APPENDIX D

SELECTED FRAUD SCHEMES

The following fraud schemes are described for illustrative purposes only.

Bustout

A bustout scheme can take many different forms. The basic approach is for an apparently legitimate business to order large quantities of goods on credit, dispose of those goods either through legitimate or illegal channels, and then close shop, absconding with the proceeds and leaving suppliers unpaid.

Bustout schemes are often perpetrated by individuals soon after the formation of a new company or through the takeover of an existing company, and are accomplished as follows:

1. Credit is established with numerous vendors, and initial payments are made promptly. Vendors therefore feel comfortable with the company and extend existing credit lines.
2. The perpetrators build inventory by ordering everything possible from vendors (regardless of the type of products) and promising to pay soon, then ordering more merchandise.
3. The perpetrators sell the inventory at deep discounts or move it to another related business before vendors can repossess it.
4. The business fails or just closes and, perhaps, files bankruptcy unless creditors take preemptive legal action.

Check Kiting

Check kiting, one of the more common types of employee embezzlement, involves the transfer of money between bank accounts and the improper recording of these transfers. In check kiting, the perpetrator takes advantage of the "float" period, which is the time between the date the check was deposited and the date that the funds are collected. The perpetrator deliberately uses the same funds in two or more banks to build apparently large balances. Check kiting can involve numerous banks and checks. The more banks and broader geographical distance involved, the harder it is to control check kiting.

Kickback

The Anti-Kickback Enforcement Act of 1986 defines a kickback as anything of value provided improperly to obtain or reward favorable treatment in connection with contract actions. In the commercial sense, kickbacks are the giving or receiving of anything of value to influence a business decision, without the employer's knowledge and consent.

A kickback is a form of off-book fraud. Off-book refers to those schemes in which the funds used for illegal payments or transfers are not drawn from the regular company bank account of the payer and the payments do not appear on the payer's books and records. If the employee responsible for the purchasing function of company is receiving kickbacks, the company usually is paying more than competitive prices for products or services. The financial statements may reflect reduced net income, as well as overstated inventory values.

Lapping

Lapping is one of the most prevalent types of internal fraud relating to accounts receivable. Lapping is a method of concealing a defalcation wherein a customer's payment is recorded sometime after payment receipt. The general lapping scheme is as follows: Cash or a bank check received from a customer is appropriated by the employee. At a later date, funds received from a second customer are credited to the first customer's account, and the second customer's account is credited still later by funds received from a third customer. As a result, there is a delay of credits, namely lapping. The lapping will continue until the fraud is detected, the funds are restored, or the scheme is covered up, for example, by a credit to the proper customer and a fictitious charge to operating accounts.

Lapping schemes may involve fund diversions to an employee's personal use or to pay other expenses to keep the business operating. Often, a lapping scheme involves falsification of documents to conceal the misappropriation of funds.

Ponzi

A Ponzi or pyramid scheme is usually any venture wherein earlier investors are repaid principal plus interest with funds provided by later investors. There may or may not be a legitimate business purpose for the venture, but the need for capital creates and continues the scheme. Often, unusually high investment returns or other inducements are offered by the promoters to attract investors.

Each Ponzi scheme typically shares three common characteristics:

1. The business activity depends on outside investor money.

2. The investor money is not used according to the stated purpose. Some of the investor money is used to pay the returns promised to earlier investors.

3. The business enterprise lacks profits sufficient to provide the promised returns and, therefore, depends on an ever increasing supply of investor money.

