2018

# The Importance and Implications of Forensic Accounting in the Financial World

Mackenzie Hitchcock
*Long Island University*, Mackenzie.Hitchcock@my.liu.edu

# The Importance and Implications of Forensic Accounting in the Financial World

An Honors Program Thesis

by

Mackenzie Hitchcock

Spring 2018

School of Professional Accountancy

_____

Michael Abatemarco, advisor

_____

Carol Boyer, reader

_____

# Table of Contents

# Abstract

This thesis thoroughly explores fraud and the forensic accounting profession. It details the education, training, and careers of forensic accountants; and why demand for this profession has suddenly spiked. The necessary skills of forensic accountants and why these skills are valuable is explored; a need for better education and training is also proposed. It also details popular forensic accounting methods and how these may be used to detect fraud. This thesis explains several fraud schemes and famous frauds that were contributors to the growing demand of forensic accountants. The fraud triangle and other contributing factors are explored.

This thesis also emphasizes the importance of strong internal controls and explains the COSO internal control framework; several important internal controls are listed and explained. Cybersecurity is also explained; including why it has become an absolute necessity and how businesses can better enforce cybersecurity measures. This thesis also explains the changes that were made following the Enron and WorldCom scandals and details the Sarbanes-Oxley Act of 2002. Explanations for the relevant changes and why they were necessary are included. The purpose of this thesis is to demonstrate the importance of forensic accounting and to thoroughly explain the facets of fraud and forensic accounting.

# Introduction

Forensic accounting is a relatively new career field that has expanded rapidly since its inception. It is now widely demanded and is continuing to grow. But why? Several events and developments have prompted this change in the financial world. Forensic accountants are highly talented individuals who possess thorough knowledge in several areas. These areas include general accounting principles, the law, criminal behavior, frauds, and computerized systems. This once random combination of skills has been made necessary by several high-profile frauds and accounting scandals that led to billion-dollar losses—and even the loss of several lives. People take money seriously and personally; it is both our means of survival and our key to luxury. There are endless incentives for employees and managers to take advantage of a flawed system. And for years, they have. Before the financial world was so big—and before technology was so advanced—fraud was not such a big issue. But because corporations now control trillions of dollars and wield a great amount of power—it is. It is the responsibility of forensic accountants to detect frauds and to protect the assets of common people.

There are many types of frauds, including Ponzi schemes and social media frauds, that affect normal people. These people may be unaware of the warning signs and probably do not have the necessary knowledge or skills to realize that they have been duped. Forensic accountants are responsible for recognizing red flags and ending frauds before they become big enough to significantly impact large numbers of people. This was not done in the case of several high-profile scandals. Some early scandals included Enron and WorldCom—the bankruptcy of these two companies was sudden and unexpected, given the success that their financial statements boasted. The Bernie Madoff Scandal and the financial crisis of 2008 were reminders

of the harm that can be done by fraud. These events prompted an increase in the demand for forensic accountants. These events also prompted sweeping changes in the way accountants and auditors do their work. The Sarbanes-Oxley Act of 2002 was the first step in correcting the flaws that had led to the Enron and WorldCom accounting scandals. Accounting regulatory boards have continued to improve standards and practices since these events and will continue to do so as new issues come to light.

Internal controls and management behavior have become increasingly important issues. Weak internal controls and a lack of emphasis on ethical behavior greatly increase the likelihood of fraud. Accountants have recognized this, and auditors and forensic accountants have appropriately adjusted their focus to emphasize the importance of strong internal controls. The COSO internal control framework centers around this issue and lays the groundwork for a good system of internal control. Technological advancements have also prompted an increase in cybersecurity. Several companies—including Equifax—have learned the hard way about the importance of cybersecurity. Forensic accountants are trained to recognize deficiencies in both internal control and cybersecurity—and are also well-versed on how to address these weaknesses.

The culmination of these issues and discoveries has led to the current state of accounting and forensic accounting. The field of forensic accounting will continue to grow and develop as more accounting and technological changes are made; and likely, as more frauds are discovered. Until then, it is important that forensic accountants are well-educated and well-trained, because thousands of innocent people rely on them every day, whether they know it or not.

# Forensic Accounting

## What is it?

The word forensic means “belonging to, used in, or suitable to courts of judicature or to public discussion and debate.” Forensic accounting, therefore, means “the use of accounting skills to investigate fraud or embezzlement and to analyze financial information for use in legal proceedings.” The forensic accounting profession developed out of a desire from accountants to “become more than simply ‘the people who did the books’” (Aldridge). Accountants and accounting firms have increasingly expanded their services to include many professional roles. Experienced accountants with “expertise in the investigation of fraud” are known as forensic accountants. Forensic accounting requires specialization in data analytics, investigative techniques, and the accounting process. Forensic accountants are responsible for identifying fraud and misrepresentation, and often must testify in court. It is important that they collect sufficient evidence to support their findings. Forensic accountants have become greatly needed in the aftermath of the financial crisis and several high-profile accounting scandals.

Forensic accountants provide services in the following areas: “business valuations, divorce proceedings and matrimonial disputes, personal injury and fatal accident claims, professional negligence, insurance claims evaluations, arbitration, partnership and corporation disputes, shareholder disputes, civil and criminal actions concerning fraud and financial irregularities, and fraud and white-collar crime investigations” (Peshori). Forensic accounting can be separated into two categories: litigation services and investigative services. Litigation services “recognize the role of an accountant as an expert consultant” (Houck et al.). Investigative services require the analytical skills of forensic accountants and may also require

testimony. Forensic accounting is “the intersection between accounting, investigation, and the law” (Houck et al.).

## What is Fraud?

Fraud refers to “wrongful or criminal deception intended to result in financial or personal gain.” It “includes all the multifarious means human ingenuity can devise that are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth” (Houck et al.). There are two types of accounting fraud: fraudulent financial reporting and misappropriation of assets. Fraudulent financial reporting is perpetrated by management and refers to the purposeful manipulation of financial statements; it is characterized by a “lack of honesty and transparency in reporting.” Management may falsely increase revenues or decrease expenses to make a company look more successful. Fraudulent financial reporting may also be utilized to achieve consistency for several years of financial data. Incentives to alter financial statements are ever-present, and many managers feel pressure to materially alter their statements to appeal to investors and creditors. Misappropriation of assets is perpetrated by employees and refers to the wrongful use of company assets for personal gain. This may occur when an employee steals inventory items or uses company money to pay his/her personal cell phone bill. Other examples of common frauds include Ponzi schemes, advance fee frauds, affinity schemes, and others.

## Why does Fraud Occur? The Fraud Triangle

The three components that make fraud possible are opportunity, attitude, and incentives/pressures. Incentives and pressures give employees and management a reason to commit fraud. Incentives include financial interests and bonuses that may be contingent on

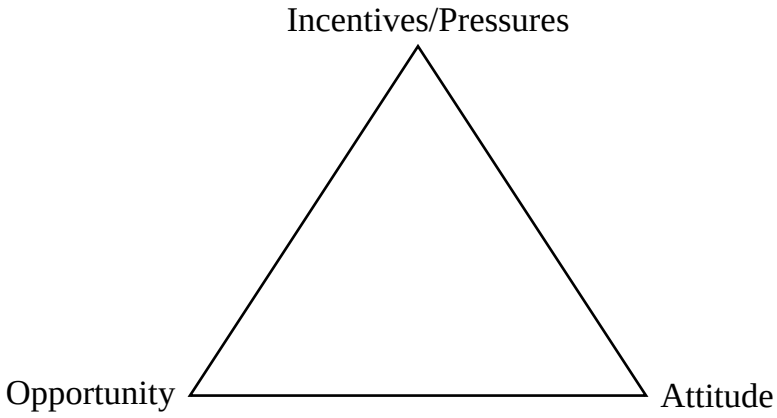
company performance. Employees may be influenced by greed when confronted with these incentives. Managers who have a large stake in the company may purposely manipulate financial statements to increase their earnings per share. Companies should avoid offering bonuses for financial performance. This can be an incentive for managers to manipulate earnings on the financial statements. Managers and employees may also be influenced by pressures. Managers of failing companies may feel pressure to lie about their revenues or profits. Employees may fear the loss of their job if they do not perform to certain standards—this pressure may cause them to falsify records.

There must also be opportunity for fraud to occur. Opportunity refers to weak internal controls or other weaknesses that make it possible for fraud to occur. Poor internal controls provide an *opportunity* for the manipulation of financial data. Forensic accountants and auditors must assess a company's internal controls before performing an audit. Weak internal controls call for a more intrusive investigation; the weaker the control, the more likely there is fraud (Ramaswamy). A company with rigid internal controls and an environment of ethical behavior is not a likely place for fraud to occur.

The third component of fraud is attitude. Fraud is more likely to occur when a company has poor corporate governance. "Corporate governance is the system of rules, practices and processes by which a company is directed and controlled" ("Corporate Governance"). It refers to the environment of a company that is instituted and controlled by upper management. It is sometimes referred to as the "control environment" or the "tone at the top". Management behavior and emphasis on ethical behavior is an important factor in preventing fraud. The attitude that is conveyed by management makes its way to the lower-level employee and dictates how the company is run. Vinita Ramaswamy says that "an increasing number of researchers are

finding that poor corporate governance is a leading factor in poor performance, manipulated financial reports, and unhappy stakeholders." It is the responsibility of management to take internal controls seriously and to convey an environment of honesty. Companies with poor corporate governance tend to spurn internal controls—this means that two of the three fraud factors are likely present.

These three components are referred to as the fraud triangle (as seen below):




## The Forensic Accounting Process

The forensic accounting process is very similar to that of the auditing process. Forensic accounting encompasses many of the elements of auditing—the distinctive difference is that auditors look for misrepresentations, whether accidental or purposeful, and forensic accountants look specifically for fraud. The first step in a forensic accounting investigation is to meet with the client and accept the job. It is important that the accountant consider whether he has the necessary skills and experience to complete the task. An accountant with no experience in casinos and gambling should probably not take a case involving a casino. Generally accepted auditing standards (GAAS) require that auditors and forensic accountants have the necessary

knowledge to competently complete a job. If an accountant lacks knowledge in a certain area, he has a chance to remedy the deficiency. He can learn, or he can hire an expert to assist in the investigation. The forensic accountant must also ensure that he is completely independent from the client and has no bias that will hinder the investigation. This is also required by GAAS. Forensic accountants may also consider other factors before accepting a job. These may include client reputation or extent of the fraud; if the accountant does not feel comfortable with the situation, he will not accept the job.

Once the job has been accepted, the forensic accountant should form "an initial action plan". This is a basic plan that will help him complete a more detailed plan later—like an outline. He will consider the client and its environment—including nonfinancial information. He will also perform analytical procedures to determine the focuses of his investigation. Analytical procedures are quick calculations pertaining to financial statement data. They often involve ratios (such as debt to equity ratio and return on sales). He will also consider internal controls and other deficiencies that make fraud more likely. It is important to both study and *test* internal controls. His findings will be used in the development of a detailed plan. It is important that the plan is developed in consideration of the goals of the investigation and the likely areas of fraud.

After a detailed plan has been developed, the accountant must carry out the investigation. Gathering and analyzing evidence is the next step. The accountant will focus on certain areas as determined by the analytical procedures and his detailed plan. He may analyze certain accounts or transactions that he deems suspicious. He will focus heavily on the areas affected by weak internal controls. He will also consider any red flags that are observed during the investigation. It is important that he keep records of his findings, because he will likely have to testify in court and will need to show evidence. The investigation is concluded with an investigative report and

advice for preventing further issues. If the case involves legal issues, the accountant will testify as to his findings (Peshori).

## Differences Between Auditing and Forensic Accounting

Forensic accounting and auditing are very similar; they have similar processes and similar methods. But they also have many differences. The first of these differences is the underlying objective. Auditors intend to detect material misstatements in financial data. These misstatements may occur due to error *or* fraud and are likely large enough to sway the decision of an investor or creditor. Immaterial matters are of little concern to auditors. Though small misstatements will be pointed out to management and the audit committee, they are not cause for an auditor to change his/her opinion on the financial statements. Forensic accountants specifically look for fraud (not errors) and may be concerned with what seem like unimportant amounts. Many frauds start small and grow into massive scandals. Early detection is key.

Forensic accounting jobs are typically conducted on a case-by-case basis and are nonrecurring. Companies *choose* to hire forensic accountants in the case that a fraud is suspected or discovered by management. Audits are recurring. Financial statement audits are required yearly for publicly traded companies. The techniques of forensic accountants and auditors also differ in some respects. The investigations of auditors are "conducted primarily by examining financial data" (SBN Staff); whilst forensic accounting investigations involve more complex analytical skills and investigative techniques. Forensic accountants must be more knowledgeable in areas such as law and criminology. They are often skilled in interrogation techniques and reading body language. This assists in detecting misrepresentations by management or other employees. Auditors may detect fraud in their work but are less likely to do so than forensic

accountants. This is because fraudsters tend to hide their work and auditors are not typically trained to detect this kind of behavior and/or deceit. This is what makes forensic accounting unique and valuable in an era dominated by fraud.

# The Education and Training of Forensic Accountants

## Important Skills

Forensic accountants are expected to possess many skills. These include the ability to be analytical, inquisitive and intuitive, ethical, skeptical, and detail-oriented. They often spend long hours looking at large amounts of information and must be adept at noticing details. They must also have a good understanding of the accounting process. This allows them to better understand financial statements and to analyze where suspicious activity has occurred. It is important that they have "a thorough understanding of fraud schemes, including but not limited to asset misappropriations, money laundering, bribery, and corruption" (Ramaswamy). Forensic accountants are also expected to understand internal controls; they must be able to analyze internal controls and give suggestions for improvement.

Forensic accountants must have a good understanding of the law and are expected to possess satisfactory communication skills; this is important because they often must testify in court. Many forensic accountants are talented interviewers and/or interrogators with an extensive knowledge of psychology. Forensic accountants must often ask questions of management and employees during investigations. They must be able to ask the proper questions and accurately interpret the responses. Many forensic accountants are skilled at reading body language and can

tell when someone is being dishonest. Investigative work is a substantial part of forensic accounting.

"Computer skills and understanding financial software" are also important ("Forensic Accounting"). This is because most accounting is done electronically. Forensic accountants must understand the software of their client and how fraud may be perpetrated electronically. Online banking and the internet have made electronic fraud extremely common. Understanding cybersecurity has become extremely important.

## Education

There are several educational paths that aspiring forensic accountants can pursue. One option is to earn a bachelor's degree in forensic accounting; this is not a common path because very few schools offer a bachelor's degree in forensic accounting. Examples of universities with a forensic accounting bachelor's degree program include: West Virginia University Institute of Technology, Embry-Riddle Aeronautical University, Waynesburg University, and Franklin University. Another option is to major in accounting, finance, or economics and to earn a certificate in forensic accounting. This is the most popular route currently. Many forensic accountants graduate with an accounting degree and earn their CPA licensure before pursuing a certificate in forensic accounting. It is also possible to earn a bachelor's degree in accounting and to pursue a master's degree in forensic accounting. Examples of universities with a forensic accounting master's degree program include: Florida Atlantic University, Southern New Hampshire University, and Stevenson University. Many of the master's degree programs are online. Students may also find it helpful to take elective courses in the following areas: business

law, criminology, ethics, psychology and statistics (“Forensic Accounting”). These will help hone their industry knowledge and relevant skills.

## Certificates

There are several certificates that forensic accountants may choose to earn. Almost all forensic accountants are Certified Public Accountants (CPAs). Another important certification is the Certified in Financial Forensics (CFF) credential. This credential is offered by the American Institute of Certified Public Accountants (AICPA). Another credential offered by the AICPA is the Accredited in Business Valuation (ABV) credential. There is also a Certified Forensic Accountant (CFA) credential offered by the American College of Forensic Examiners International (ACFEI) and a Certified Fraud Examiner (CFE) credential offered by the Association of Certified Fraud Examiners (ACFE). Forensic accountants may also choose to pursue the Certified Valuation Analyst (CVA) or Accredited Valuation Analyst (AVA) credentials. These are both offered by the National Association of Certified Valuation Analysts (NACVA). The Forensic CPA Society offers a Forensic Certified Public Account (FCPA) credential and the National Association of Forensic Accountants (NAFA) also offers a credential (“Forensic Accounting”). Accountants may choose to earn one or more of these credentials on their way to becoming a successful forensic accountant.

## Training

Most forensic accounting training is on-the-job training. Many forensic accountants begin their careers in tax or auditing and use their experiences in these fields to develop their forensic accounting skills. Auditing closely resembles forensic accounting—auditors are responsible for detecting material misstatements in financial statements. The key difference is that auditors look

for both mistakes and fraud whilst forensic accountants look specifically for fraud (not mistakes). Some firms focus specifically on forensic accounting and hire accountants directly out of college. These forensic accountants begin directly in the forensic accounting field and receive on-the-job training specific to forensic accounting.

## Where and How Forensic Accountants Work

Demand for forensic accountants has increased drastically since the 2008 financial crisis. Big companies and financial institutions have realized how devastating fraud can be; and now understand the benefits of detecting fraud early. There has been a push for better education and training for forensic accountants because the supply of forensic accountants is not currently on par with the increasing demand. It is estimated that 35% of the market share of forensic accounting is provided by Big Four accounting firms. Much of the remaining demand is satiated by small forensic accounting companies.

Law enforcement agencies (such as police forces) may also choose to hire forensic accountants. They can do so in one of three ways: in-house employment, temporary relocation, or outsourcing. Each way has benefits and drawbacks. In-house employees are the cheapest of the three and ensure increased security; but they "can be difficult to attract" and cannot give an expert opinion. The second option is hiring on temporary reassignment. Forensic accountants that are hired on temporary reassignment may have "access to other support, such as technical and corporate intelligence." This type of support is more flexible; and accountants that are hired on temporary reassignment may be more "up to speed on current accountancy issues" (Aldridge). Hiring forensic accountants in this way may be less advantageous than hiring in-house employees because it is more expensive and may result in higher employee turnover. The third

option is outsourcing. This is typically the most expensive option; and security may become an issue. But outsourced support may increase the speed of an investigation, and outsourced forensic accountants are able to provide an expert opinion. Outsourcing (though typically the most expensive) may prove to be less expensive if forensic accounting services are rarely needed (Aldridge). Law enforcement agencies must consider each of these factors in deciding how to hire their forensic accounting staff.

## Ideas for Improvement

It is important that forensic accountants have the necessary knowledge and skills to adequately complete their investigations. Accountants that are not well-prepared may find themselves overwhelmed and incompetent. A planning panel and a technical working group at West Virginia University were tasked by the National Institute of Justice with developing a "model curriculum" for forensic accountants. They specified that entry-level forensic accountants should have knowledge in criminology, the "legal, regulatory, and professional environment", ethical issues, fraud issues (including fraud in a digital environment), and "forensic and litigation advisory services" (Houck, et al.). Having a solid background in these areas will help forensic accountants to more effectively complete their jobs.

As demand for forensic accountants increases, more universities should consider offering a forensic accounting major. Forensic accounting classes may help accountants to be better prepared for their future careers. Universities should also emphasize the importance of taking other relevant classes (such as law or data analytics). It is also important for forensic accountants to utilize their experiences in the fields of auditing and tax; understanding the relevance of general accounting knowledge is essential for success. The researchers at West Virginia

University also emphasized continuing professional education in their model curriculum (Houck, et al.). This is important because the fields of finance and accounting are constantly changing; and it is important to understand relevant technological issues in these areas.

# Forensic Accounting Techniques

## Analytical Procedures and Ratio Analysis

Analytical procedures are performed by both auditors and forensic accountants. One of the most common analytical procedures—and one of the most common ways to identify fraud—is ratio analysis. Ratio analysis is simple—accountants compare ratios to determine whether they are likely or unlikely. If the ratio is unlikely, the area should be investigated more thoroughly. The ratio may be compared to financial data from prior years or to the industry average. Any significant change or difference may be an indicator of fraud. There are six different categories of ratios.

The first category is liquidity ratios. Liquidity ratios measure the ability of a company to meet its short-term obligations. The following are liquidity ratios:

Current Ratio = Current Assets/Current Liabilities → this ratio measures the company's ability to pay its current liabilities with its current assets

Quick Ratio = (Current Assets - Inventory)/Current Liabilities → this ratio measures the company's ability to pay its short-term debt with its liquid assets

Working Capital = Current Assets - Current Liabilities → this measures the company's use of its assets and liabilities in its day-to-day operations

The second category is activity ratios. Activity ratios measure how effectively a company uses its assets. The following are activity ratios:

Accounts Receivable Turnover = Net Credit Sales/Average Net Accounts Receivable → this ratio measures the company's effectiveness at collecting receivables

Number Days Receivables = 365/Accounts Receivable Turnover → this ratio measures the number of days it takes for the company to collect its receivables

Inventory Turnover = Cost of Goods Sold/Average Inventory → this ratio measures how quickly inventory is sold

Number Days Inventory = 365/Inventory Turnover → this ratio measures the number of days inventory spends in stock before being sold

Fixed Asset Turnover = Net Sales/Net Fixed Assets → this ratio measures how effectively a company utilizes its fixed assets

Total Asset Turnover = Net Sales/Average Total Assets → this ratio measures how effectively a company utilizes its total assets (fixed and current)

The third category is leverage ratios. Leverage ratios measure how effectively a company uses its debt to finance its assets and operations. The following are leverage ratios:

Debt Ratio = Total Debt/Total Assets → this ratio measures a company's debt in relation to its assets

Debt to Equity Ratio = Total Liabilities/Common Stockholder's Equity → this ratio measures a company's debt in relation to its equity

Times Interest Earned = Net Income before Interest and Taxes/Interest Expense → this ratio measures a company's cost of debt

Cash Flow Coverage = (Earnings Before Income Taxes + Lease Payments + Depreciation)/Average Total Assets → this ratio measures a company's ability to pay its financial obligations with its cash flows

Leverage = Average Total Assets/Average Common Stockholder's Equity → this ratio measures a company's assets in relation to its equity

The fourth category is profitability ratios. Profitability ratios measure a company's ability to generate revenue. The following are profitability ratios:

Return on Sales = Net Income after Taxes/Sales → this ratio measures the percent of a company's sales remaining after expenses and taxes have been paid

Return on Assets = Net Income/Total Average Assets → this ratio measures how efficiently assets are used to generate income

Return on Common Equity = (Net Income After Interest and Taxes - Preferred Dividends)/Average Common Stockholder's Equity → this ratio measures the return on common stock

Number of Times Bond Interest Earned = Net Earnings after Income Taxes/Bond

Interest Expense → this ratio measures a company's income in relation to its bond interest

Number of Time Preferred Dividends Earned = Net Earnings after Income Taxes/Preferred Dividends → this ratio measures a company's income in relation to its preferred stock dividends

The fifth category is growth ratios. Growth ratios measure the change in the growth of the company. The following are growth ratios:

Earnings per Share = Net Earnings Available to Common Stockholders/Weighted Average Number of Outstanding Common Shares → this ratio measures the earnings/return per share of common stock

Payout Ratio = Cash Dividends/Net Income → this ratio measures a company's ability to pay dividends

Dividend Yield = Dividend per Share/Current Market Price per Share → this ratio measures the rate of return per share in terms of dividends

The sixth category is valuation ratios. Valuation ratios measure the company's ability to provide shareholder value. The following are valuation ratios:

Price to Earnings = Current Market Price per Share/Earnings per Share → this ratio measures investors' willingness to pay for a company's equity

Book Value per Common Share = Common Equity Book Value/Shares Outstanding → this ratio measures a company's net worth

Market to Book = Market Price per Share/Book Value per Share → this ratio represents investors' opinions about the company and its ability to generate profit/returns

Earnings Yield on Common Stock = Earnings per Share/Current Market Price per Share → this ratio measures the earnings yield on common stock (Rosner, Auditing, Analytical Procedures & Common Ratios, 3/23/18)

## Direct/Transaction Method

The Direct Method of forensic accounting is also known as the Transaction Method. This method involves examining "canceled checks and invoices, contracts, agreements and public records and notices" (Kent). The accountant will also likely interview management and employees; this gives a better understanding of the accounting process and where there is potential for fraud. Examining all relevant documents ensures that the investigation is conducted thoroughly. The forensic accountant will also prepare a working statement of cash flows to better understand the inflows and outflows of cash; and where there may be suspicious gaps or unknown transactions.

## Cash T Method

The Cash T Method is conducted by comparing the amount of cash received to the amount of cash spent. The purpose of this method is to "determine if a company or individual had understated income" (Kent). It is often used when sources of income are not clear; or it is likely that income was purposely excluded from the financial statements. This method is especially useful in divorce litigation. It is common for moneymaking spouses to attempt to hide

their true net worth during divorce proceedings to cheat their spouse out of money. It is the job of the forensic accountant to determine the spouse's sources of funds and true net worth.

This method is conducted by listing all known sources and uses of cash. It is important to remember that this method only considers *cash* transactions. All cash receipts are listed as debits; and all cash expenditures are listed as credits. This method is useful when the forensic accountant can *accurately* determine personal expenses. After determining all cash receipts and expenditures and totaling them together, the forensic accountant can calculate unidentified income by subtracting receipts from expenditures.

Cash Expenditures – Cash Receipts = Unidentified Income

If this equation results in a zero balance, then there is no unidentified income and it is unlikely that fraud has occurred. But if unidentified income is discovered, the forensic accountant should do further work to identify the sources of this income ("Cash Intensive").

## Source and Application of Funds Method

The Source and Application of Funds Method is similar to the Cash T Method. This method "examines the amount spent on lifestyle versus assets and investments" (Kent). This is another useful way to determine the net income and true worth of an individual or company. This method does *not* only consider cash transactions; it also considers "changes in assets and liabilities." Sources of cash include "decreases in assets, increases in liabilities or nontaxable receipts" and applications of cash include "increases in assets, decreases in liabilities and nondeductible expenses" ("Cash Intensive"). Because beginning and ending account balances are required to perform this method, it is more time-consuming than the Cash T method. It is much easier to apply this method if a statement of assets and liabilities (or a balance sheet) is available

for use. After all sources and applications have been identified, total sources are subtracted from total applications to identify any understatement in adjusted gross income.

Cash Applications – Cash Sources = Understatement of Adjusted Gross Income

## Net Worth Method

The Net Worth Method is conducted by subtracting net liabilities from net assets to determine net worth. This is reliant on the basic accounting equation:

Assets = Liabilities + Owner's Equity

Net worth is then "compared to reported income over several periods" (Kent). Any strange differences are a red flag to forensic accountants and should be investigated further. Forensic accountants may also calculate the change in net worth over several years to identify any discrepancies ("Cash Intensive").

Change in Net Worth = Ending Net Worth – Beginning Net Worth

This calculation can be tricky because fair market value is not always equal to GAAP (generally accepted accounting principles) value. The appraisal of assets may be subjective; and this may cause discrepancies between book value and true net worth. It is helpful to practice conservatism when using this method. This method is also useful in divorce proceedings. A forensic accountant may compare calculated net worth to reported net worth; large differences may be a sign of fraud.

## Bank Deposit Method

The Bank Deposit Method is another way of comparing cash in to cash out. This method "compares the total deposits plus cash expenses minus nontaxable sources of income to the total receipts shown on the return" ("Cash Intensive"). This method is most useful when the taxpayer deposits *all* receipts in the bank and the forensic accountant is able to *accurately* determine expenses. The equation for this method is as follows:

Net Deposits + Undeposited Cash Expenditures = Total Receipts ("Cash Intensive")

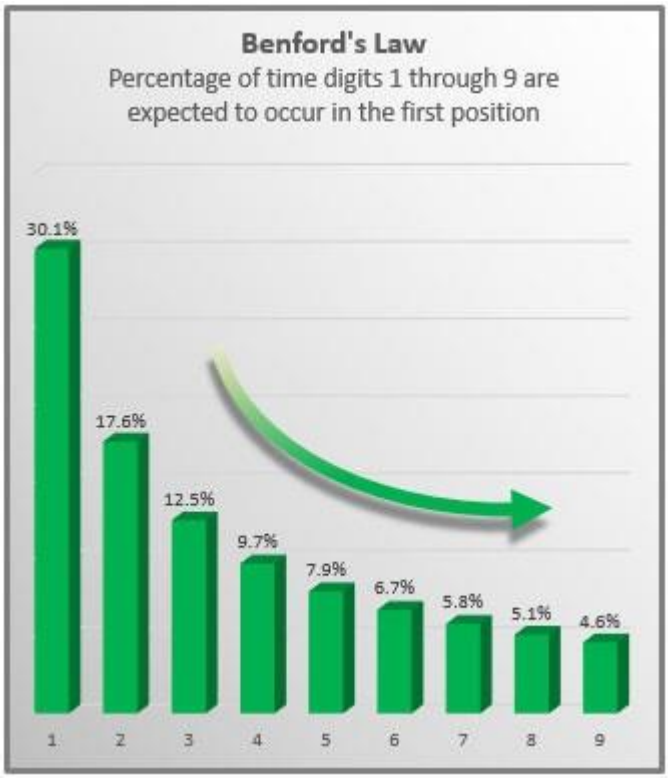
Net deposits equal all bank deposits minus nontaxable income. Nontaxable income may include pensions, gifts, loans, and any other nontaxable sources of income (regardless of whether deposited). Cash expenditures is calculated by subtracting checks written from total expenditures. Checks written can be determined by subtracting ending bank balances from beginning balances plus deposits.

Checks Written = Beginning Bank Balances + Deposits – Ending Bank Balances

## Benford's Law

Benford's Law is "a statistical tool to determine whether the data under study shows any pattern signifying suspicious movement" (Peshori). Frank Benford assigned probabilities to each digit in a number; these probabilities represented the likelihood that the numbers were "naturally occurring (or nonfabricated)" (Collins). The law states that the number 1 "will be the leading digit in a genuine data set of numbers 30.1% of the time" (Collins). The probability corresponding to the number 2 is 17.6%; and the probability corresponding to the number 3 is

12.5%. The probability of each number steadily decreases. The visual representation of this pattern is known as Benford's curve. The following image depicts this law:



(Collins)

Benford's Law may allow a forensic accountant to calculate the *probability* of fraud; but Benford's Law is not used to *detect* fraud (Peshori). An accountant may use Excel to analyze a set of numbers and to compare the proportions of leading digits to the probabilities assigned by Benford's Law. Significant discrepancies between the predicted probabilities and the true occurrences may be an indicator of fraud. Benford's Law is more effective when used with a large data set—data sets of at least 500 numbers are more likely to conform to Benford's Law than smaller data sets. It is also important that each digit has an equal *chance* of occurring. Data sets in which certain numbers are more common are not well-suited to this analysis. For example, a "company that charges its customers either $49.99 or $79.99" would not have data suitable to this kind of analysis (Collins).

## Theory of Relative Size Factor (RSF)

Relative Size Factor (RSF) is the ratio of the largest number in a set of data to the second largest number in the set.

$$\text{RSF} = \frac{\text{Largest Record in a Subset}}{\text{Second-Largest Record in a Subset}}$$ ("Relative Size Factor Test")

The purpose of the RSF test is to identify any outliers or inconsistencies in data that may indicate fraud ("Relative Size Factor Test"). The RSF test is performed on "subsets" of data. Purchase data may be grouped into subsets by vendor; these vendor subsets can be used for an RSF test. "The test identifies subsets where the largest amount is out of line with the other amounts for that subset" ("Relative Size Factor Test"). This may occur if the data actually belongs to another subset; it may also occur if an amount has been improperly recorded. This can happen because of error or fraud and should be investigated further. RSF may also be calculated over several periods and examined for "unusual fluctuations" (Peshori). Fluctuations may be an indicator of fraud.

# Types of Frauds

## Ponzi Scheme

A Ponzi scheme is a pyramid scheme in which money from new investors is given to old investors in the form of "returns". The original investors give a sum of money that is "invested" in the market. The perpetrator of the fraud makes promises of high returns with little risk. But the money is not actually invested; it is kept by the perpetrator of the Ponzi scheme. As this

perpetrator deceives new investors and receives new investments, he/she uses these "investments" to pay returns to the previous investors. The scheme continues to grow as the perpetrator obtains new investors and investments. He/she often keeps portions of the investments for him- or herself. The fraud continues to grow as new investors join. Each "level" of the scheme requires a larger number of investors to repay the former investors. It is unlikely that the scheme can go on forever. The perpetrator will eventually run out of new investors and the pyramid will collapse. Investors are left without returns *and* their initial investments.

A Ponzi scheme has several indicators. One indicator is the promise of "high returns with little or no risk" ("Types of Fraud"). This promise is counterintuitive—investments with high returns typically require higher risk; and low-risk investments mean lower returns. Overly consistent returns are another sign of a Ponzi scheme. It is unlikely that a true investment will yield the same or closely similar returns over a long period of time. Investment returns typically follow the market at least generally—returns that spurn market trends and remain consistent over time may not be true "returns".

Unregistered investments and unlicensed sellers are also signs of a Ponzi scheme. True investments will be recorded with the SEC; and state and federal law requires licenses for those who sell investments. Paperwork issues can be another indicator. True investments will typically have reliable paperwork. Ponzi schemes do not involve actual investments and therefore do not have proper paperwork. Investors should also be wary of overly complex investment strategies; strategies that seem overcomplex and difficult to understand may be a cover for the lack of real investing. Investors may be confused or intimidated by an overly complex strategy and may be discouraged from asking questions. Perhaps the most indicative sign of a Ponzi scheme is trouble

withdrawing money ("Types of Fraud"). The most famous Ponzi scheme in history is the Bernie Madoff Ponzi scheme.

## Affinity Scheme

An affinity scheme is a fraud that is carried out within a specific group. An investment might be presented to a certain group as "exclusive"; this ensures that the group feels connected. Group members often do not turn to the police or the SEC when this type of fraud is perpetrated because they do not wish to take the matter outside of the group. Often, perpetrators of this fraud trick group leaders into becoming complicit in the fraud. They may convince group leaders that the investment is trustworthy and worthwhile; when group leaders present the investment to group members, the members are more likely to participate. Affinity schemes are often Ponzi schemes that are conducted within a smaller segment of society ("Types of Fraud").

## Advance Fee Fraud

An advance fee fraud involves the prepayment of an "advance fee." This fee is paid for some sort of deal to go through. It may involve "the sale of products or services, the offering of investments, lottery winnings, found money, or many other so-called opportunities" ("Types of Fraud"). The perpetrator of an advance fee fraud may target investors who have previously lost money in investment schemes or desire to sell underperforming securities. The fraudster may offer to sell these securities for the investor after an "advance fee" is paid. The fraud may seem legitimate because the perpetrator will ask the investors to wire money to escrow agents or lawyers. They may also use "official-sounding websites and e-mail addresses" ("Types of Fraud"). They then keep the advance fee and disappear before performing the promised service.

## Pump and Dump Scheme

Pump and dump schemes are relatively simple. They involve true investments but rely on false information. The conductor of a pump and dump scheme will typically boast about a stock and will encourage other investors to buy shares quickly. This increases the price of the stock. This part of the fraud is known as “pumping”. When the stock price has been “pumped” to the desired level, the conductors will sell their stock. This is known as “dumping”. The conductors sell their stock at the newly-created higher rate and make money, whilst the other investors are left with shares that quickly drop in price (“Types of Fraud”).

## Internet and Social Media Fraud

Internet and social media frauds are carried out through the internet. These types of frauds are low cost and easily “reach a mass audience” (“Types of Fraud”). Fraudsters may send legitimate looking e-mails to dupe investors. These e-mails may include links to phony websites. When investors click on these links, they are routed to a website that asks them to enter personal information. They may think that they are entering this information on a legitimate website, but they are really sending their information to the perpetrator of the fraud. Similarly, fraudsters may use social media to conduct fraud. They may create tweets or Facebook statuses with links that look legitimate (“Types of Fraud”). It is important for internet users to be aware of these types of frauds and to be sure that the links they are following are legitimate. Online transactions are subject to fraud and hacking. This has created a need for better cybersecurity.

# Famous Frauds

## The Enron Scandal

The Enron Scandal occurred because of fraudulent financial reporting. The management of Enron altered its financial statements to reflect positive operating results and returns; when in reality, the company was going bankrupt. It collapsed in 2002. This fraud was perpetrated by the management of Enron and the auditors of the Enron financial statements. The auditor for Enron was Arthur Andersen. Arthur Andersen was a "big five" accounting firm at the time of the fraud; the company has since ceased to exist. This fraud would not have been possible without the compliance of Arthur Andersen—had the auditors done their job properly, the fraud would have been discovered long before the company went bankrupt.

This fraud was carried out and covered up in several ways. Perhaps the most alarming way in which Enron concealed this fraud was by failing to release certain required financial statements. Publicly traded companies are required to release five financial statements: a balance sheet, an income statement, a statement of stockholder's equity, a statement of cash flows, and a statement of comprehensive income (this was not required at the time of the fraud). Notes to the financial statements must also be released. For almost six years, Enron did not release a balance sheet with its yearly financial statements. In the third quarter of 2001, the company *only* released an income statement. This increased suspicion and accelerated the downfall of Enron.

The management of Enron continually ignored generally accepted accounting principles in the preparation of its yearly financial statements. Arthur Andersen auditors failed to identify this. By avoiding GAAP and through the formatting of certain transactions, Enron was able to turn a 2001 "$618 million net loss…into $393 million in net income" (Barrett). Specifically, they

were able to do this by excluding certain “nonrecurring” transactions. They also excluded certain related party transactions from their notes and failed to disclose the amounts of contingent liabilities. Enron had very poor corporate governance and an unethical tone at the top.

One of the most startling aspects of this fraud was the lack of independence between Enron and Arthur Andersen (the auditor). Auditors are required to be independent from their clients—this reduces the possibility of audit failure. Because Arthur Andersen was doing non-audit work for Enron (like tax returns and consulting), they were not independent. In fact, they made *more money* on their non-audit work than they did on their audit work. “When non-audit fees comprise a substantial piece of an auditor’s income from the audit client, those fees might tempt an auditor to overlook an enterprise’s ‘aggressive’ accounting simply to retain the client’s non-audit business” (Barrett). The discovery of this lack of independence led to sweeping changes in generally accepted auditing standards and the way in which auditors are monitored. It is now illegal for CPA firms to perform non-audit services for their audit clients.

## WorldCom

WorldCom was, at one point, the second largest long-distance phone company in the United States. In 2002, the company, whose financial statements boasted billions in profits, filed for bankruptcy. It was found that the company had misled investors and creditors by participating in fraudulent financial reporting. The CEO, Bernard Ebbers, was sentenced to 25 years in prison for his role in the scandal. The CFO, Scott Sullivan, was sentenced to five years in prison; he received a reduced sentence for pleading guilty and testifying against Ebbers. The downfall of WorldCom resulted in the laying off of 17,000 workers.

The management of WorldCom was able to alter their financial statements by incorrectly capitalizing $3.8 billion in operating expenses. This allowed them to spread the expenses over several years and to boost their yearly profits. This is not allowed under generally accepted accounting principles—something that should have been noted by their auditors. The company also made "transfers between internal accounts of $3.06 billion in 2001 and $797 million in the first quarter of 2002" ("WorldCom"). These transactions also did not conform to GAAP. The auditor for WorldCom, Arthur Andersen, maintained that they were not informed about the internal transfers and did not discuss the accounting treatment of those transfers with the management of WorldCom ("WorldCom"). WorldCom now operates under the name MCI, Inc. and is a subsidiary of Verizon. Many people found it suspicious that Arthur Andersen was the auditor for both Enron and WorldCom and the independence of the auditors was called into question.

## The Bernie Madoff Scandal

Bernie Madoff was a stockbroker and investment advisor who ran a multi-billion-dollar investment firm called Bernard L. Madoff Investment Securities, LLC. The firm was found in 2008 to be nothing but an enormous Ponzi scheme and is now considered the largest financial fraud in history (worth $65 billion). Madoff was able to deceive investors and employees and even his own family—they were all convinced that he was a successful investor. He held many important leadership positions in the financial world—he was the chairman of NASDAQ and head of the National and International Securities Clearing Corporations. His sons worked for him for over twenty years and were unaware of the ongoing fraud. Madoff had been perpetrating the fraud since 1991; in 2007, he ran out of money. The fraud was collapsing and he had no way to pay his investors. He was forced to turn himself in (*The Wizard of Lies*).

Madoff had not intended for the fraud to be malicious—he thought that he would be able to end it on his own but found himself digging a deeper hole. The only person who knew of "the nature of the operation" was a loyal employee named Frank. He knew how to fake trades and make the investments look real. He also thought that Bernie would be able to make his way out of the fraud. They were both wrong. Madoff fooled and defrauded millions of investors—and many people lost their homes and life savings. A few committed suicide (including one of Bernie's sons). Bernie was jailed for life. Frank also went to jail for his involvement (*The Wizard of Lies*).

Many were fooled by this scheme—but one man was not. A chief investment officer named Harry Markopolos was one of the few people who was suspicious of Bernie Madoff Investments. He discovered the fraud long before it collapsed. The methods he used were simple—he analyzed market trends and compared them to the performance of "investments" made by Bernie Madoff. One of the biggest red flags was the clear lack of correlation between Madoff's investment performance and the performance of the S&P 500 (the market in which he was supposedly investing). He realized that the returns earned by Madoff's investments were improbable (if not impossible); and concluded that Madoff was not being honest with his investors. The returns on Madoff's investments were much too consistent and often spurned market trends. These are common signs of a Ponzi scheme. Markopolos wrote multiple letters to the SEC explaining the suspected fraud and urging an investigation, but his concerns were ignored (United States, Congress, House, 2009). Had his concerns been taken seriously, the fraud may have been identified sooner, and the losses may have been limited to a smaller amount. Harry Markopolos is now a forensic accountant.

## The 2008 Financial Crisis

The 2008 financial crisis occurred as a result of mortgage-backed securities being sold to investors at a AAA rating when in reality they were backed by unreliable mortgages. This is because of collateralized debt obligations (CDOs). CDOs are bonds that are composed of hundreds of debt instruments (such as mortgages). CDOs may be composed of some AAA rated loans and some B loans; but if there is enough diversity, the CDO will receive a good rating. Investors did not realize that there were risky mortgages packaged with the reliable mortgages in which they were investing. These securities were reliable at first; but banks eventually ran out of credit-worthy individuals to offer mortgages to. They turned to low-credit individuals who were unlikely to pay off their mortgages (*The Big Short*).

One man was able to recognize this and successfully predicted the downfall of the economy. Michael Burry ran an investment firm called Scion Capital and argued to his investors as early as 2005 that the mortgage market would collapse "in the second half of 2007" (Burry). He made his prediction based on research he conducted "into the residential mortgage market and mortgage-backed securities" (Burry). He found that many people were defaulting on their mortgages but that bond prices continued to go up. Burry said, "I had watched as these mortgages were offered to more and more subprime borrowers—those with the weakest credit. The lenders generally then sold these risky loans to Wall Street to be packaged into mortgage-backed securities, thus passing along most of the risk. Increasingly, lenders concerned themselves more with the quantity of mortgages they sold than with their quality… the incentive for fraud was great." He realized that CDOs were deceiving and that they were likely to fail. Burry did more research to confirm his suspicions and found that the fraud was much more extensive than he had previously assumed. He realized that there was a housing bubble that was

doomed to burst. He decided to buy credit-default swaps. Credit-default swaps are a type of insurance on bonds; this means that when bonds fail, owners of credit-default swaps make money. In essence, Michael Burry bet against the American economy. Burry made 200:1 returns when the market collapsed (*The Big Short*).

Banks were the major perpetrators of this fraud. They sold the CDOs to investors and refused to revalue them when it was clear that they no longer had value. It is unclear whether they did not know how to rate the bonds or they purposely swindled bondholders. The rating agencies (S&P 500, Moody's, etc.) were competing for business. They did not want to devalue the loans because they would lose business. They continued to label CDOs with AAA ratings when it was clear that the bonds were backed by risky mortgages. Eventually, the market crashed. Investors lost billions and many banks collapsed. Several large banks required bailouts during the financial crisis. The 2008 crash collapsed the entire world economy (*The Big Short*).

Mary E. Barth and Wayne R. Landsman researched the generally accepted accounting principles that may have contributed to the financial crisis (i.e. what principles may have led to the deception of investors). They studied the financial reporting of banks to draw their conclusions. Barth and Landsman concluded that fair value accounting likely played little role in the financial crisis but that disclosures related to securitizations and derivatives were likely insufficient. Had there been more detail included in the disclosure notes relating to these subjects, investors may have been able to make better informed decisions about the "values and riskiness of affected bank assets and liabilities" (Barth and Landsman). They note that the Financial Accounting Standards Board and the International Accounting Standards Board have since taken steps to correct this deficiency.

## Equifax

The Equifax hack occurred as the result of a data breach that exposed the information of more than 145.5 million consumers. The CEO of Equifax explained that the hack occurred because of "both human error and technology failures" (Hendry). The technology failure occurred in an application called "Adobe Struts" that was used in Equifax's online disputes portal. The human error occurred when the problem was not addressed by the IT department. Equifax had discovered the technological deficiency on March 8, 2017 and had asked the IT department to correct the vulnerability. It was never corrected, and a later security scan failed to detect the vulnerability. It is thought that the fraud was perpetuated for almost five months before the program was shut down.

This case highlights the importance of cybersecurity and its relevance to the field of forensic accounting. Internal controls and cybersecurity help prevent technological failures and data breaches such as the one that occurred at Equifax. This is the first step in deterring frauds such as identity theft. Forensic accountants must often deal with cybersecurity and the frauds related to its failure. They are also responsible for identifying the deficiencies in internal control that could result in fraud.

# Internal Controls

## Types of Internal Controls

There are several types of internal controls that are important in the prevention of fraud. One of the most important internal controls is segregation of duties. Segregation of duties

ensures that employees do not have an opportunity to commit fraud *and* to cover it up. There are four basic functions that should be separated. These include: authorization, recording, custodial, and reconciliation.

Authorization refers to the approval of an action and is usually performed by a manager. Most lower-level employees cannot enter their own hours or approve a return of merchandise without manager authorization. Recording refers to data entry; any employee who records transactions or other information participates in data entry. This often includes recording the receipt of invoices or checks. The custodial function is performed by employees who have *physical access* to assets. Employees that are responsible for handling inventory or customer checks participate in the custodial function. The final function is reconciliation. Reconciliation may refer to bank statement reconciliations or the reconciliation of receipts with ledger entries. Employees who perform the reconciliation function are responsible for checking that all data matches with real transactions. The segregation of these four functions ensures that employees do not have an opportunity to both perpetrate fraud and cover it up. This makes it much less likely that employees will attempt to commit fraud.

There are also many other internal controls that can be applied to prevent fraud. One of these is prenumbered checks. Prenumbered checks allow managers and auditors to easily check for missing or duplicate checks. This type of control is called a sequence check. Forensic accountants may perform a sequence check because stolen or missing checks may be an indicator of fraud. Duplicate checks may also be a red flag. Forensic accountants can also do sequence checks for other documents. Invoices and shipping orders should also be prenumbered. Missing checks or invoices may be a sign that assets have been stolen or misappropriated; and duplicate documents may be a sign that management is fraudulently increasing revenue. Forensic

accountants typically use auditing software to perform sequence checks because it is quicker and more accurate.

A type of control that also doubles as a cybersecurity measure is an access control. Access controls are simple—they ensure that only authorized users can access sensitive information. Users that have permission to access private data are given usernames and passwords. Outsiders do not have the proper access codes and cannot access protected data. Access controls are not foolproof because managers typically can override them. Outside hackers may also find ways to bypass this security measure.

Companies should also perform regular physical audits and reconciliations to ensure that their records are accurate. Performing these audits regularly ensures that fraud is detected early. Employees may also be deterred from participating in fraud if they are aware of regular inventory and bank account reconciliations. Preparing trial balances is a similar way to prevent fraud. Ensuring that both sides of the accounting equation are equal throughout the financial year can prevent unexpected surprises or mistakes. This may help in the early detection of financial statement frauds.

## Steps for a Successful System of Internal Control

The Committee of Sponsoring Organizations for the Treadway Commission (COSO) developed a "model for evaluating internal controls" in 1992 (Cruz). This model is known as the COSO cube; this is because the model looks like a Rubik's cube. The front of the model displays the five steps for successfully implementing a system of internal controls. These steps are as follows:

1. Control Environment: This is also sometimes referred to as the “tone at the top”. The control environment refers to the attitude of management regarding internal controls. It is important that management establishes a strong ethical environment and displays ethical behavior. Internal control is more successful when management abides by the system and makes it known that internal controls are important.
2. Risk Assessment: Risk assessment refers to the evaluation of risks within the company. Management must determine what the riskiest areas are so that they can design an effective system of internal controls. Internal controls should be applied more heavily to riskier areas.
3. Control Activities: Control activities refer to the controls set by management. These are the actual internal controls that are designed and implemented. They should be designed in consideration of the likely areas of fraud and the riskiest areas as determined by management.
4. Information and Communication: Information and communication refer to the process of informing lower-level employees about the controls and how to effectively use them. Internal controls are pointless if *all* employees cannot effectively abide by them. Proper training and literature regarding internal controls should be provided to employees.
5. Monitoring Activities: It is important that internal controls are continuously monitored by management for any weaknesses or ineffectiveness. Management should determine whether areas of risk have changed or whether the controls are being effectively used by all employees to ensure that fraud does not occur. Controls should be modified if they are not effective (Cruz).

The top of the model displays the objectives of internal controls:

1. Operating: The operating objective refers to "the effectiveness and efficiency of the entity's operations" ("COSO—Control Environment"). Operating controls are intended to regulate the daily operations of the business. It is the goal of management to implement internal controls that align with the operating effectiveness of the business. Controls that place a burden on employees or the company may not be worthwhile controls. Controls that are outrageously expensively are also not worthwhile. Controls should be efficient; and the benefits of internal controls should outweigh the costs.
2. Reporting: The reporting objective refers to "the financial or non-financial reporting's reliability, timeliness, transparency or other terms" ("COSO—Control Environment"). A company should have internal controls over its reporting processes—this is to ensure that fraudulent financial reporting does not occur; and that non-financial reports are accurate and reliable.
3. Compliance: The compliance objective refers to "the entity's adherence to the laws and regulations it is subject to" ("COSO—Control Environment"). These controls are implemented to ensure that all relevant laws and rules are followed. Applicable laws/regulations should be considered in the designing of internal controls.

The right side of the model displays the relevant areas of internal control application:

1. Entity Level: Controls should operate effectively across the entire company. Entity level controls are strongly affected by corporate governance. A strong ethical environment constitutes a strong entity level system of internal controls.
2. Division: Internal controls should also be applied at the division level. A division is a distinct part of a business; and the business is responsible for the actions and reporting of

each division. Divisions may also be responsible for the actions and reporting of operating units.

3. Operating Unit: An operating unit is a subsidiary of a business that has its own assets and liabilities. Each operating unit should have a strong system of internal control; if the financial statements of an operating unit are incorrect, then the financial statements of the entire business will be incorrect.
4. Function: Internal controls should apply to each function of a business. Small tasks like recording and depositing checks should be dictated and monitored by internal controls. Small mistakes can add up to big mistakes; and internal controls at the function level ensure that small mistakes are minimized.

The COSO cube appears as follows:


(Cruz)

The cube is designed this way to demonstrate that there is intersectionality between internal controls, the parts of a business, and the business' objectives. Each part of the cube should be considered when designing a system of internal control.

# Cybersecurity

## What is it?

Cybersecurity has become extremely important in the wake of several high-profile data hacks. Forensic accountants often deal with cybersecurity because they are responsible for reporting on weaknesses that create a potential for fraud. Weaknesses in computer software and security create a high potential for hacking and fraud. Cybercrime is "the use of digital tools by criminals to steal or otherwise carry out illegal activities" (Singer and Friedman). Most crimes today involve a digital component and may be considered cybercrime.

A cybersecurity issue occurs when an outside party attempts to interfere with the technology of a company. Simple errors and mistakes are not considered cybersecurity issues; and interference by an outside party is only considered a cybersecurity issue if the outside party has malignant intentions. "A cyber problem only becomes a cybersecurity issue if an adversary seeks to gain something from the activity, whether to obtain private information, undermine the system, or prevent its legitimate use" (Singer and Friedman). There are three goals of cybersecurity: confidentiality, integrity, and availability. These are sometimes called the "CIA triad" (Singer and Friedman).

Confidentiality refers to protecting company and customer information. Trade secrets and personal data are valuable and can be used by hackers for personal gain. Even information that seems irrelevant can have valuable meaning and should be protected. Confidentiality can be achieved through the use of access controls and encryption. Legal protections may also be used.

Integrity refers to the accuracy of data. Data that is altered without authorization loses its integrity. It is important that companies can trust the information they are using. Hackers may

find it profitable to change the information in a company's system; they may even alter programs so that they perform incorrectly while appearing to perform correctly. "Integrity's subtlety is what makes it a frequent target for the most sophisticated attackers" (Singer and Friedman). Hacks affecting integrity are often overlooked but may cause the most devastation.

Availability refers to the ability to use computers and programs as expected. Availability is compromised when computers or programs shut down without warning and users are unable to complete necessary tasks. These attacks are often known as DDoS attacks. DDoS stands for distributed denial-of-service. Hackers perform this type of attack by overcrowding a server and causing it to shut down; the server is then unavailable to true users. This type of attack is often threatened in what is known as a "ransomware" attack. This involves a threat to the availability of a system; and a demand for ransom money in return for not executing the attack. Hackers may use this type of attack to gain control of a system. The ultimate goal of a cyberattack is to gain access to and control over the entire system. This is known as "root access" and occurs when "the attacker has the ability to execute any command" or "the victim is completely vulnerable" (Singer and Friedman).

## Common Types of Cybercrime

The most common types of cybercrimes are those involving the "misuse of account details to defraud financial and payment systems" (Singer and Friedman). This type of fraud is known as credential fraud. Hackers may be able to steal account details such as usernames and passwords from stores and other sources that store user information. This data can be used to hack into credit card or online banking accounts; and to steal money. Companies have a

responsibility to keep customer data safe; they can be liable for data hacks that expose the personal information of their customers.

Hackers can also steal this information directly from the customer. This is done through internet and social media fraud. Hackers can send fake emails with links to dangerous websites. These often look very real; and users can become easily confused. It is important that customers are wary of suspicious emails. Customers should always check the email address of the sender and should be careful when following links. Fake emails are known as “phishing” emails (Singer and Friedman).

Cybercriminals attempt to trick their victims into giving money willingly. They do so by targeting “our most basic human emotions: greed, fear, and love” (Singer and Friedman). They may target greed by offering a get-rich-quick scheme. This is like an advance fee fraud. The hacker may offer large returns in lieu of a small payment; but the victim makes a payment and the returns never come. They may also create pop-up windows that offer prizes or rewards; when users click on these fake offers, they are prompted to enter personal information. This information can then be used by the hacker for financial gain.

Cybercriminals may also use fear to steal information. They may create fake pop-up windows that warn of viruses and other dangers. These pop-ups include a link to “download antivirus software”—but this is really a link to download malware. Users should be careful when warning messages appear on their computers; these messages are often fake and can cause more harm than good.

The third way that cybercriminals steal information is through love. Cybercriminals may hack into emails or social media accounts and use these platforms to send a plea for help. They

often claim to be a stranded traveler in immediate need of money. Victims often send money to help their "stranded" family member or friend; but this money is received by the hacker. Hackers may also send out fake nonprofit emails. This strategy is popular after a recent tragedy. Unwitting users may donate money to the fake charities; and this money is taken by the hackers.

Hackers may also target businesses by blackmailing them. Cybercriminals may threaten to hack into a company's database or to disrupt a company's flow of business if not given a "ransom" payment. This is known as a ransomware attack. Companies often pay the criminals because the loss they would suffer otherwise is greater. This type of cybercrime may also affect customers. If businesses refuse to make the "ransom" payment, it is likely that customer information will be stolen, or business will be interrupted. This hurts both the company and its customers. It is extremely important that companies install hefty protections and make reasonable decisions when confronted with this type of cybercrime.

Another way that cybercriminals gain access to a system is through the manipulation of lower-level employees. This is perhaps the easiest way for a hacker to achieve their goal. A common scheme is to call a lower-level employee and pretend to be a manager or technical support assistant. The employee is inclined to believe the caller (as they have been told it is their superior) and is likely to reveal sensitive information over the phone—such as a username and password. This information can then be used by the hacker to access a protected system. Hackers may also use blackmailing to frighten these employees. They may threaten to reveal sensitive or embarrassing personal information if not given the access codes. These tactics are known as "social engineering" (Singer and Friedman). Phishing emails fall under this category. Humans are the weakest link in cybersecurity. It is often misplaced trust that leads to a larger

cybersecurity issue. All employees and forensic accountants should be trained in cybercrime and cybersecurity to minimize human error.

## Preventing Cybercrime

One of the easiest ways to protect against cybercrime is by using complex and secure passwords. Most people use common words or phrases that can be easily guessed by hackers. The most common passwords are “password” and “123456” (Singer and Friedman). Many people use simple passwords because they are easier to remember. Writing passwords down and storing them in a secure location can help expedite this problem. Many services now require a certain password complexity. Most online banking portals, for example, have password requirements. These may address length, the use of both lowercase and capital letters, and the use of special characters (*, &, !, #, $, %, @, etc.). Companies and individuals can work together to create more secure passwords.

It is also the individual responsibility of internet users to exercise caution. Users should be wary of emails from unknown sources (and even emails that look legitimate). Users should also be aware of cybercrime schemes and should make educated decisions when addressed with a possible scam. Companies should also conduct training regarding cybercrime and how to address possible scams. Management attitude about cybersecurity is similar to management attitude about internal control. It is important that management emphasizes safe internet practices and the importance of protecting secure information. Like internal control weaknesses, cybersecurity weaknesses should be promptly addressed. Delaying the repair of issues can lead to serious security breaches. Many hacks occur over several weeks or months; and could have been prevented if weaknesses were addressed sooner. This is what occurred at Equifax.

# Steps Toward a Better Future

## The Sarbanes-Oxley Act of 2002 and the Public Company Accounting Oversight Board

Several changes were made following the collapse of Enron and WorldCom. The Sarbanes-Oxley Act was passed in 2002 under the leadership of President George W. Bush. The Sarbanes-Oxley Act (often known as SOX) was intended to protect investors from potential frauds. One of the biggest measures taken in the Sarbanes-Oxley Act was to establish the Public Company Accounting Oversight Board (PCAOB). The PCAOB is composed of five members appointed by the SEC. These members can serve no more than two five-year terms and only two of the five can be CPAs. The PCAOB is responsible for establishing standards relating to the audits of public companies. All auditors of public companies must register with the PCAOB and are subject to inspections by the PCAOB. The PCAOB can regulate and discipline CPA firms that do not conform to the standards set by the PCAOB.

## Generally Accepted Auditing Standards

The standards created by the PCAOB are known as Generally Accepted Auditing Standards (GAAS) and are as follows:

General Standards—these standards apply to the auditors:

- Auditors must have adequate technical training and proficiency
- Auditors must maintain an independence in mental attitude
- Auditors must always exercise due professional care

Standards of Fieldwork—these standards apply to the audit:

- Auditors must adequately plan and properly supervise the audit
- Auditors must have a sufficient understanding of the entity and its environment, including internal control; this information should be used to design and implement the audit
- Auditors must obtain sufficient appropriate audit evidence to provide a reasonable basis for their opinion

Standards of Reporting—these standards apply to the auditor's report:

- The audit report must state whether the financial statements are presented in accordance with GAAP
- The report must identify circumstances in which GAAP has not been *consistently* applied
- The report must ascertain that informative disclosures (notes to the financial statements) are adequate unless stated otherwise in the report
- The report should clearly state the degree of responsibility being accepted by the auditors by expressing an opinion or stating that an opinion cannot be expressed

## Prohibited Services

The PCAOB has prohibited auditors from performing certain non-audit work for their audit clients. These services are as follows: bookkeeping, financial systems design and implementation, investment services, certain tax services, internal audit outsourcing, management/HR functions, actuarial services, appraisal or valuation services, and legal and expert services. Auditors cannot perform these services for their clients because each of these services hinder their independence.

Auditors cannot perform bookkeeping for their clients because it would be a form of self-review—the auditors would be auditing the financial statements that *they* prepared. Auditors also cannot perform appraisal or valuation services; this is because auditors often must evaluate the appraisals/valuations made by their clients. This would also be a form of self-review. Similarly, auditors cannot perform actuarial services or internal audit outsourcing for their clients. They are also prohibited from designing and implementing financial systems for their clients; this is because they may not be able to find the flaws in internal control for systems that they have designed. This may increase the likelihood of an audit failure.

Auditors also cannot perform investment services or legal and expert services for their clients. Performing these services for audit clients would create a conflict of interest. Lawyers are expected to be advocates for their clients; auditors who perform legal services for their clients would be too involved in the well-being and success of the client. This would undermine their independence. This is also why auditors cannot perform management or human resource functions for their client—they may become too invested in the success of the company. This would greatly impair their independence. Auditors who perform investment services for their clients may also lose independence. They may feel obligated to push the envelope on certain transactions to maximize profit for their clients—this would conflict with the policy of conservatism practiced by auditors. Auditors are also prohibited from performing certain tax services that may interfere with their independence; however, most standard tax services are not prohibited.

## Recent Changes to the Auditor's Report

The PCAOB recently made changes to the format of the auditor's report that will take effect this year (for any companies with a fiscal year ending on or after December 15, 2017). These changes include the following:

1. The auditor's report must now include a discussion of "critical audit matters" (CAMs). Critical audit matters include any matters that are reported to or are required to be reported to the audit committee *and* that
    a. Relate to material accounts or disclosures *and*
    b. Involved especially challenging, subjective, or complex auditor judgement (Rosner, Auditing, Auditor's Reports, 2/15/18)

    Determining which matters should be classified as critical audit matters is subjective; auditors will have to consider the matter and its complexity. There are several disclosures that must be made in relation to critical audit matters. The auditors must disclose the matter, a description of *why* the auditors determined that it was a critical audit matter, a description of how the matter was addressed during the audit, and a reference to the related financial statement accounts and disclosures (Rosner, Auditing, Auditor's Reports, 2/15/18). The purpose of the change is to ensure that financial statement users are fully aware of the issues that arose during the audit and how these issues were addressed. The users may find this information helpful when considering the amounts presented in the financial statements.

2. The auditor's report must now specify that it encompasses both the financial statements *and* the accompanying notes to the financial statements. This provides more clarity for

financial statement users. Because certain transactions and contingencies are required to be disclosed, it is important that financial statement users are aware that the notes have been audited.

3. The auditor's report must state in which year the auditor began consecutively auditing the client (i.e. an auditor that has audited the same company since 2013 would have to specify that they began consecutively auditing the client in 2013). This change was made to ensure that auditor independence is not compromised. Some fear that auditors may become too comfortable with long-term clients. Disclosing the year in which they began working for a client ensures that financial statement users can make knowledgeable judgements about auditor independence or lack thereof.
4. The auditor's opinion will be stated at the *beginning* of the report. This is simply to make the report easier to read; the user can easily find the most important piece of information.

## The Importance of Forensic Accounting

Forensic accounting has become a well-known and widely demanded field. The Enron and WorldCom scandals opened the public's eyes as to the dangers of fraud and the likelihood that it goes undetected. The financial crisis of 2008 and the Bernie Madoff scheme reminded Americans and many people around the world that fraud is ever-present and can dangerously affect shareholders. It is clear that more must be done to prevent these scandals. The Sarbanes-Oxley Act of 2002 was designed to prevent fraud; and though it has increased the transparency of reporting and the independence of public auditors, more must be done. Forensic accountants should be utilized more frequently. Frauds that go undetected until bankruptcy have the potential

to hurt millions of people. The prevention and early detection of fraud is essential to protect the assets of common Americans.

Corporations have three goals after discovering a fraud has been committed: “first, to identify the fraudster, secondly to secure the evidence to legally terminate their contract, and thirdly to make sure it cannot happen again” (Aldridge). Forensic accountants have been trained in each of these areas. They can identify and detect fraud and are trained to collect relevant evidence. Forensic accountants are also able to give helpful suggestions for future fraud prevention. Their skills are unique and highly necessary in a financial world that is constantly at risk.

# Conclusion

There are many events that have contributed to the increasing demand for forensic accountants. Famous financial statement frauds like the Enron and WorldCom scandals prompted legislation and sweeping changes to financial reporting. The financial crisis of 2008 and the Bernie Madoff scandal brought new fraud schemes to light; and the Equifax scandal emphasized the importance of cybersecurity. These failures startled the public and have prompted an increase in the demand for forensic accountants. The growth of big business and the advancement of technology have further increased the need for better controls over financial reporting. The public has become more educated about fraud and the potential dangers involved in investing. As these frauds have been discovered and the demand for forensic accountants has grown, the field of forensic accounting has grown and improved accordingly.

Forensic accountants are highly skilled and well-trained to recognize fraud in a variety of ways. Their competence in accounting, law, criminology and fraud makes them well-equipped to recognize and end fraud schemes. Current education options are limited, though some schools do offer degrees in forensic accounting. Most forensic accountants begin their careers in tax or audit and use this experience to eventually pursue forensic accounting. Most forensic accountants also have some sort of certificate that qualifies them for the position (such as Certified Fraud Examiner). It is important that we continue to improve these education and training opportunities to ensure that future forensic accountants are well-prepared to adequately perform their jobs.

It is also important that businesses continue to implement strong systems of internal control and that an environment of ethical behavior is maintained. These are both strong factors in deterring fraud. Strong internal controls ensure that employees cannot easily commit frauds that go undetected. Cybersecurity is another important control measure that has become extremely important in today's technological world. The Equifax scandal was a devastating example of what can happen when cybersecurity is not properly implemented and maintained. It is important to realize that cybersecurity and internal control failures can affect innocent people. Businesses have a responsibility to protect their stakeholders by deterring fraud.

Though there are many things that must still be improved, we have made great strides toward preventing fraud. The Sarbanes-Oxley Act of 2002 and subsequent changes to financial reporting and auditing standards have greatly improved the reliability of financial reporting. Auditor independence has been thoroughly addressed and is still being improved. Regulatory boards such as the PCAOB continue to make important changes to auditing standards that help to ensure that fraud and misstatements do not go undetected. Forensic accounting continues to grow and improve. The public is beginning to recognize the importance of this career field and the

work that is done by forensic accountants. It is imperative that the field continues to grow and improve as new developments are made and new issues are discovered.

# Works Cited

Aldridge, Roger. “The Crime-Fighting Accountants: Roger Aldridge Explains the Role of Forensic Accountants in Tackling Fraud and Organised Crime.” *Policing Today*, Sept. 2008, p. 22+. *Criminal Justice Collection*, go.galegroup.com/ps/i.do?p=PPCJ&sw=w&u=nysl_li_liu&v=2.1&id=GALE%7CA19347456&it=r&asid=673458edf2937a2560cbdac24ddc9d28. Accessed 7 Sept. 2017.

Barrett, Matthew J., Enron, Accounting and Lawyers. Notre Dame Lawyer, pp. 14-20, Summer 2002. Available at SSRN: https://ssrn.com/abstract=782365

Barth, Mary E., and Wayne R. Landsman. "How did Financial Reporting Contribute to the Financial Crisis?" *European Accounting Review*, vol. 19, no. 3, 7 July 2010. *Taylor & Francis Online*, www.tandfonline.com/doi/full/10.1080/09638180.2010.498619?scroll=top&needAccess=true. Accessed 20 Nov. 2017.

*The Big Short*. Directed by Adam McKay, Paramount, 2015.

Burry, Michael J. "I Saw the Crisis Coming. Why Didn't the Fed?" *The New York Times*, 3 Apr. 2010, www.nytimes.com/2010/04/04/opinion/04burry.html. Accessed 19 Nov. 2017.

"Cash Intensive Businesses Audit Techniques Guide -- Chapter 5 -- Examination Techniques." *IRS.gov*, Internal Revenue Service, www.irs.gov/pub/irs-utl/cashchapter5_210639.pdf. Accessed 23 Apr. 2018.

Collins, J. Carlton. "Using Excel and Benford's Law to Detect Fraud." *Journal of Accountancy*, Association of International Certified Professional Accountants, www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html. Accessed 1 Apr. 2018.

"Corporate Governance." *Investopedia*, www.investopedia.com/terms/c/corporategovernance.asp. Accessed 30 Mar. 2018.

"COSO--Control Environment." *Deloitte.*, Deloitte Touche Tohmatsu Limited, www2.deloitte.com/ng/en/pages/audit/articles/financial-reporting/coso-control ojectenvironment.html. Accessed 8 Apr. 2018.

Cruz, Sharise. "What are the Five Components of the COSO Framework?" *KnowledgeLeader*, protiviti, 28 Oct. 2016, info.knowledgeleader.com/bid/161685/what-are-the-five components-of-the-coso-framework. Accessed 6 Apr. 2018.

DiGabriele, James A. "An Imperical Investigation of the Relevant Skills of Forensic Accountants." *Journal of Education for Business*, vol. 83, no. 6, 7 Aug. 2010, pp. 331-338.

Dr. Rebecca Rosner. Auditing Class Notes. Auditor's Reports and Analytical Procedures & Common Ratios. 15 February 2018 and 23 March 2018.

Edge, Michael Edward, and Pedro R. Falcone Sampaio. A Survey of Signature Based Methods for Financial Fraud Detection. Computers & Security, Volume 28, Issue 6, 2009, Pages 381-394, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2009.02.001.

"Forensic Accounting." *AccountingEDU.org*, www.accountingedu.org/forensic-accounting.html. Accessed 5 Dec. 2017.

"Forensic Accounting." *FBI Jobs*, Federal Bureau of Investigation, www.fbijobs.gov/career paths/forensic-accounting. Accessed 18 Sept. 2017.

Glater, Jonathan D. "Business; And Now, a Case for the Forensic Accountant." *The New York Times*, The New York Times Company, www.nytimes.com/2001/05/27/business/ business-and-now-a-case-for-the-forensic-accountant.html?mcubz=1.

Greenland, Collin A. A. "Incorporating 'Cutting Edge' Forensic Accounting Techniques/Methodologies into College/University Auditing." *Association of College & University Auditing Annual Conference*, 30 Sept. 2015.

Hendry, Erica R. "How the Equifax Hack Happened, According to its CEO." *PBS News Hour*, NewsHour Productions, 3 Oct. 2017, www.pbs.org/newshour/nation/equifax-hack happened-according-ceo. Accessed 20 Nov. 2017.

Houck, M. M., et al. (2006). Forensic Accounting as an Investigative Tool. *The CPA Journal, 76*(8), 68-70. Retrieved from http://0 search.proquest.com.liucat.lib.liu.edu/docview/212257264?accountid=12142.

Kent, Jessica. "Forensic Accounting Methods." *Chron*, Hearst Newspapers, smallbusiness.chron.com/forensic-accounting-methods-66552.html. Accessed 4 Dec. 2017.

Peshori, Kishore S. “Forensic Accounting a Multidimensional Approach to Investigating Frauds and Scams.” *International Journal of Multidisciplinary Approach & Studies*, vol. 2 no. 3, May/June 2015, pp. 26-36. EBSCO*host*, 0 search.ebscohost.com.liucat.lib.liu.edu/login.aspx?direct=true&&db=a9h&AN=108425 55&site=ehost-live&scope=site.

Ramaswamy, Vinita. "Corporate Governance and the Forensic Accountant." *The CPA Journal*, vol. 75, no. 3, 2005, pp. 68-70, *ABI/INFORM Collection*, http://0search.proquest.com.liucat.lib.liu.edu/docview/212309534?accountid=12142.

"Relative Size Factor Test." *Ebrary.net*, ebrary.net/13411/business_finance/relative_sie_factor_test. Accessed 16 Apr. 2018.

SBN Staff. "How Forensic Accounting Can Help Snuff Out Fraud and Mismanagement." *Smart Business*, Smart Business Network, 1 Dec. 2014, www.sbnonline.com/article/forensic accounting-can-help-snuff-fraud-mismanagement/. Accessed 17 Apr. 2018.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

"Types of Fraud." *Investor.gov*, U.S. Securities and Exchange Commission, www.investor.gov/ protect-your-investments/fraud/types-fraud. Accessed 7 Oct. 2017.

Tysiac, Ken. "Demand Strong for Forensic Accountants in Wake of Financial Crisis." *CPA Insider*, CPA.com, 24 Sept. 2012, www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/ Articles_2012/CPA/SEP/ForensicAccounting.jsp. Accessed 5 Oct. 2017.

United States, Congress, House, Committee on Financial Services. *Hearings*. Testimony of Harry Markopolos, CFA, CFE, Government Printing Office, 2009.

*The Wizard of Lies*. Directed by Barry Levinson, 2017.

"WorldCom." *Investopedia*, www.investopedia.com/terms/w/worldcom.asp. Accessed 2 Apr. 2018.