Proven Controls to Steer You Clear of Fraud

FFC4/23/V2

201 N. King of Prussia Road
Suite 370
Radnor, PA 19087
P : (610) 688 4477
F : (610) 688 3977
info@surgent.com
surgentcpe.com

SURGENT
ContinuingEducation

Calling All **Exceptional**
INSTRUCTORS

Surgent is currently accepting nominations

for prospective new discussion leaders in the following areas:

Tax

Accounting & Audit

Gov't and Not-for-Profit A&A

Business and Industry
(all topics)

If you are an experienced CPA with strong public speaking and teaching skills and an interest in sharing your knowledge with your peers by teaching live seminars, we would love to hear from you!

Interested in becoming a Surgent discussion leader?

Reach out to us at
recruitment@surgent.com

SURGENT
ContinuingEducation

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

SURGENT FOR ENTERPRISE

Educational Solutions That Advance the Strategic Value of Everyone in Your Firm

At Surgent, we tailor our offerings — **exam review**, **continuing education**, and **staff training programs** — to meet your organization's specific needs in the most convenient and effective ways possible.

Personalized Exam Review

Help associates pass faster with the industry's most advanced exam review courses

- Adaptive study model offered for CPA, CMA, EA, CISA, CIA, and SIE exams
- Monitor employees' exam review progress with Firm360

Continuing Professional Education (CPE)

Make CPE easy for you and your staff with several ways to buy, earn, and track CPE

- Flex Access Program – Secure a pool of CPE hours your staff can pull from in live webinar and/or self-study format
- On-Site Training – Reserve an in-firm training with a Surgent instructor
- Course Licensing – License content from Surgent to lead your own CPE training

Staff Level Training

Leverage highly practical sessions, organized into suggested curricula according to staff experience levels

- Audit Skills Training Program
- Internal Audit Training Program
- Taxation Training Program

FIRM CPE PORTAL

Track and manage CPE for all users in your organization quickly and easily with Surgent's Firm CPE Portal.

Request a demo today!

Every firm is unique — and that is why we built our customizable, innovative Surgent for Enterprise program.

Contact our Firm Solutions team today to learn how Surgent can partner with you to create a solution to support staff development for your organization.

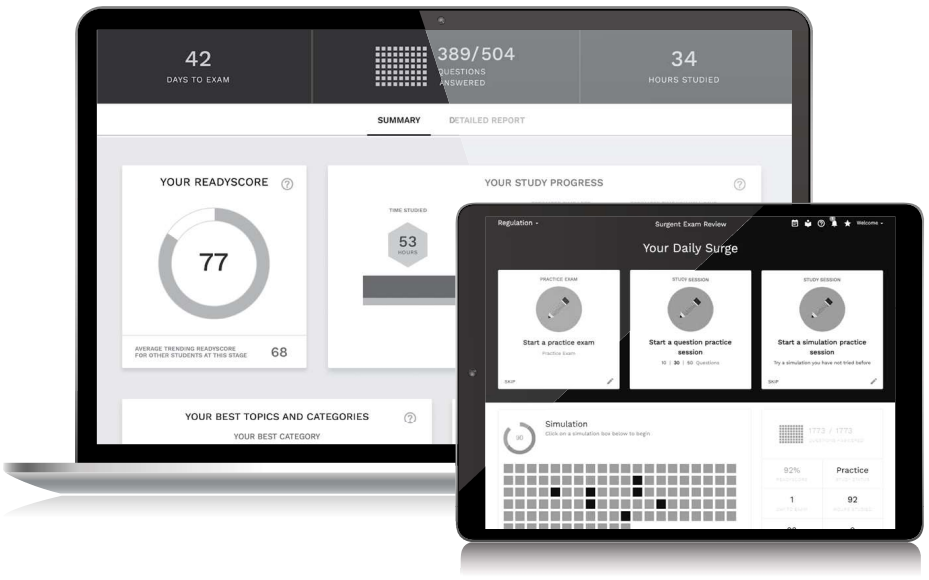
(484) 588.4197
salesinfo@surgent.com

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

STUDY LESS AND PASS FASTER

with the industry's most advanced exam prep courses

Surgent's AI-powered software personalizes study plans for each student, targeting knowledge gaps and optimizing those plans in real time. This award-winning approach has been shown to save candidates hundreds of hours in study time.



KEY FEATURES

READYSCORE

Know what you're going to score before taking the exam.

PERFORMANCE REPORTS

Leverage your dashboard to know how you're doing every step of the way.

PASS GUARANTEE

If you fail your exam after using our course, we'll refund your money.

A.S.A.P. Technology

helps you pass the

- **CPA** Exam
- **CMA** Exam
- **EA** Exam
- **CIA** Exam
- **CISA** Exam
- **SIE** Exam

Leading education for your firm? Surgent offers preferred partner pricing, coaching, and more support methods to our firm clients and their staff. **Contact our Firms Solutions team today at salesinfo@surgent.com.**

Ready to explore exam prep course packages from Surgent? **Visit surgent.com to learn more!**

Table of Contents

Revised June 2023

NOTES

Introduction

Introduction

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Understand the prevalence of fraud;
- Recognize that a perpetrator may tip their hand; and
- Understand that controls are not the panacea for fraud.

I. Age-old battle lines

Fraud plagues all organizations – large, small, public, private, for-profit, and not-for-profit. The Association of Certified Fraud Examiners (ACFE) states in the *Occupational Fraud 2022: A Report to the Nations* that all organizations lose about 5 percent of revenue to fraud each year![1]

This course will focus on the basic elements of fraud, namely the potential tip-offs that indicate someone may – emphasis on *may* – be engaged in a scheme. We will also cover some internal controls to implement to make it harder to steal.

Before we begin, it is my unpleasant task to inform you of something that you may already know but likely do not wish to face: There is at least one fraud scheme presently underway in your organization *right now*. Why am I so confident in this assertion? Many years ago, while I was working in the retail industry, I wanted to reduce inventory shrinkage. 'Shrinkage' is a euphemism for theft. Sure, there is breakage with certain inventory, but in reality, shrinkage is primarily from theft – committed by shoppers visiting the store and employees working in the store.

To make an impact, I needed to increase employees' awareness of the problem. I did not want to stand before my staff and sound accusatory. I also wanted them to become more aware of how shoplifters operate (particularly regarding expensive items). To this end, I turned to the local police department, which was more than happy to send over a detective assigned to the area where the mall was located. It was during the very first training session that the detective from the Methuen Police Department in Massachusetts shared this informational statistic from the Federal Bureau of Investigation (FBI):

Reality check 1:

If you have 10 employees, one will never steal from you; one will steal every chance they get; and the other eight will steal if they think they can get away with it!

What a stunning reality. The figures from the Association of Certified Fraud Examiners (ACFE) also lead us to believe this statement is true. Therefore, if as many as nine out of 10 employees will or may steal from an organization, then it is safe to say that every organization has at least one fraud (if not more) underway right now! We will look at data from the ACFE in a few pages, but first, let us ruminate on this fact for a while longer. What makes it even more alarming is that, based on the ACFE data, most fraudsters are engaged in multiple schemes *simultaneously*. Each scheme may include different accomplices.

---

[1] Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*. Association of Certified Fraud Examiners, p. 4. Review Chapter 4 of this course for a discussion of the controls in place at fraud victim organizations. Review Chapter 2 of companion course **DRF4** for a breakdown of other key information in the 2022 report.

II. What tips?

Our first discussion of fraud tip-offs will center around an ACFE article published several years ago on deviant behavior in the workplace. The ACFE has now incorporated data into the 2022 report on this so-called deviant behavior. Consider the similar adrenaline rush a fraudster may experience from engaging in deviant behavior and committing fraud.

We will then turn to historic schemes to see if any clues were overlooked. If there were clues, why did they go unnoticed?

III. New opportunity

About 20 years ago, organizations began reporting certain types of non-financial information in corporate social responsibility (CSR) reports. Circa 2015 (perhaps even earlier, for some), organizations started producing bigger, bolder reports covering environment, social, and governance (ESG) information. These reports include the organization's approach to and efforts toward diversity, equity, and inclusion (DEI).

Question to ponder:

Does your organization (or any of your clients' organizations) produce ESG/CSR/DEI reports?

Investors and lenders – especially *potential* investors and lenders – are placing more emphasis on a company's approach to mitigating damage to the climate. With this emphasis comes a need for an opinion regarding the truthfulness, realism, and reasonableness of these reports. As auditors, we face a huge challenge.

We will end the course with an in-depth discussion of ESG, CSR, and DEI reports. The single biggest concern for us as CPAs is our ability to audit such reports. Do we possess the scientific skills needed to review a company's greenhouse gas emissions? If a company says that it is going to reinforce plants and offices in the Midwest, specifically in the Tornado Alley region, what evidence would we need to see regarding the plans? Engineering drawings? Architectural renditions? We will certainly need to see invoices for the work. Is it enough to strengthen a building to mitigate tornado damage? Will the buildings be able to withstand an F1 tornado? (On the Enhanced Fujita Scale, this is considered a weak tornado, with wind speeds between 73 and 112 miles per hour.[2]) What about an F2 tornado, with wind speeds up to 157 miles per hour?[3] It may be necessary to enlist the assistance of subject matter experts.

Even the social aspect poses challenges. How can CPAs assess hiring practices? How can we assess diversity? Do we look around a client's offices and see diversity? Even identical twins may have different opinions on the same matters. Defining and evaluating such terms may prove difficult.

---

2 Tornado Facts & Information. "F1 Tornado - Fujita Scale." Retrieved April 14, 2022, from https://www.tornadofacts.net/tornado-scale/f1-tornado.html.

3 Tornado Facts & Information. "F2 Tornado - Fujita Scale." Retrieved April 14, 2022, from https://www.tornadofacts.net/tornado-scale/f2-tornado.html.

Deviant Workplace Behavior

Deviant Workplace Behavior

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Realize that people may act in certain ways they cannot hide while concealing fraud;
- Understand the two basic categories of "workplace deviant behavior"; and
- Recognize that some deviant behavior may have dire consequences.

I. Introduction

In the spring of 2012, the ACFE's *Fraud Magazine* published an article that truly gave me pause. Not only was the title provocative, but the text itself opened my eyes to a potentially unused tool in fraud detection. The article, entitled, "Find Deviant Behavior, Find Fraud?" was authored by Ryan C. Hubbs. Upon finishing the piece, I spoke to my co-workers in the human resources department. Sadly, they never acted beyond simply agreeing with me that Hubbs' hypothesis was fascinating. Hubbs suggests that people who engage in so-called deviant behavior in the workplace cannot hide this behavior because it is so engrained in them. However, these same people can pull off a fraud scheme and hide the scheme or schemes much better. Therefore, Hubbs postulates, if we find an employee at any level of our organization engaging in "deviant behavior" in the office environment, we may be wise to open an investigation to look for fraud.

II. Deviant behavior and fraud

A. Human drivers

Hubbs begins by stating there are three basic drivers behind human behavior: money (or other means to obtain food, shelter, and the necessities of life); sex (the drive to procreate); and power (which could be power over our environment or group). He reminds us that former senator John Edwards was accused and tried for paying his mistress to remain silent about their extramarital affair. If the news got out, Edwards feared he would likely lose his presidential bid, not to mention his seat in the U.S. Senate.[1] In this case, all three basic human drivers – money (payoff), sex (affair), and power (political) – were present. The author will go on to equate these three drivers to the three sides of the fraud triangle.

B. Concealment connection

The more Hubbs looked at certain cases, the more he wondered if there was a connection, a correlation between what would best be described as deviant behavior by any person and the commission of fraud by the same person. Recall that former Senator Edwards was accused of using campaign money to pay off his mistress. Prosecutors said that this was, for all intents and purposes, a form of embezzlement forbidden by federal campaign finance law. (Edwards was acquitted on one of six counts, and the judge declared a mistrial on the remaining five counts. The U.S. Justice Department subsequently dropped those five charges.)

[1] Edwards was acquitted on one charge; a mistrial was declared regarding the other three. The charges were subsequently dropped because the prosecution could not prove the cash payment of "hush money" was cash from campaign funds.

Could an affair between two co-workers also mean fraud was being committed by one or both people involved? After all, the intra-office affair already involves misdirection and lies. Might a power-hungry executive who circumvents policies and procedures use the same power to control others through manipulation, threats, and force?

C. The fraud triangle

Recall the fraud triangle's three elements of fraud – we will dig a little deeper below. Donald Cressey described (and Hubbs reminds us in his article) that the three sides to the triangle are motivation, opportunity, and rationalization. Curiously, Cressey was focused strictly on embezzlement by persons in positions of trust when he created the triangle. He and others later realized that these three factors must converge for any unlawful or immoral act. Let us make a brief overview of each side so we can overlay Hubbs' "deviance" factors.

"Motivation" is also referred to by some as the pressure or need to act contrary to laws, regulations, rules, or policy. When it comes to theft, there are two main sources of motivation. The first source is the inherent need to steal – the thrill, the game, or worse – a psychopathic issue. Generally, this person will steal every chance they get. The second source is the need to steal arising due to some other force – three years without a pay increase, a spouse who loses their job, increased expenses at home, the need to appear better off financially than the person really is, etc. These are the folks who will steal if they think they can get away with it. It is important to understand that the perception they will escape detection will change the more desperate they believe their situation is. For example, one may not go skydiving for fun, but faced with a plane in distress where parachuting to safety is the best option, the perception of danger and risk changes from avoidance toward doing something one would not otherwise do.

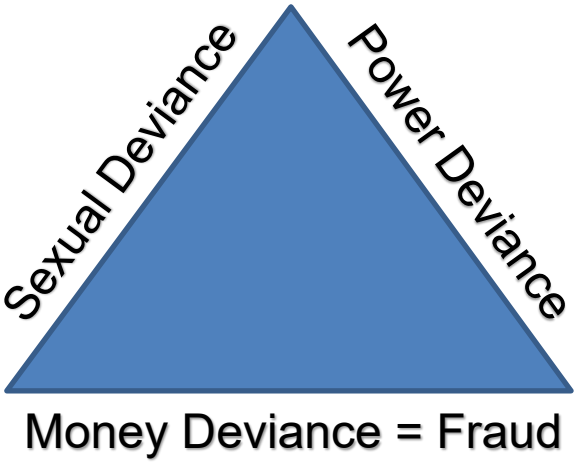
"Opportunity" simply means that there is an opening to act. This opportunity may likely present itself in weak internal controls, such as in the case of the Dixon, Illinois city comptroller who had complete authority and access with no supervision.[2] Most fraud schemes start beyond one year more than one year after the perpetrator joins the victim organization. It takes time to ascertain the best chance to steal.

"Rationalization" is how the person reconciles an illegal and immoral act with their conscience. Someone who has not had a raise in three years sees senior management receive pay hikes and bonuses and decides, "Enough! It's time I got my fair share!" It could be simply that the company has billions of dollars in revenue and a few thousand dollars diverted my way will not be missed. Perhaps scariest of all is the rationalization, "I like the feeling I get when I steal. I need to experience the feeling." Fraud becomes an addiction. (They become part of the 10 percent who will steal every chance they get.) Another rationale for stealing is that they are just *borrowing* the funds. They will repay the funds later. (They are still part of the 80 percent who steal because of their perceived need and ability to get away with it.)

[2] We will review this and other major fraud cases in the next chapter.

Hubbs then correlates these sides of the triangle to his list of primal human drivers' triangle, namely:

- Money deviance is the fraud scheme itself and ties directly to the fraud triangle;
- Sexual deviance; and
- Power deviance.



It is sexual and power deviances that may tip us off to money deviance, that is, fraud behavior. Hubbs then determined that sexual deviance might include accessing, possessing, or in any other way viewing pornographic materials. It may also be an extramarital affair or other inappropriate personal relationship between a supervisor and employee. Power deviance would include such acts as retaliation, threats, and harassment.

D. Methodology

It was time to test the hypothesis, so Hubbs turned to the internet and searched Lexis/Nexus for articles indicating fraud and deviant behavior in the workplace. Hubbs admits in the article that time was tight, so he limited his search to a three-month period. Using key words in combination, he began his search and uncovered 126 articles where fraud and some deviant behaviors were mentioned in the story. The most frequent key word link was between 'pornography' and 'fraud.' There were no instances of 'racism' and 'fraud' in his sample.

E. Results

Hubbs broke the cases into two areas: sexual deviance and power deviance. The following are examples:

Sexual deviance 1:

The CFO of a local hospital quit a $164,000 a year job after Feds notified the hospital they were investigating. "Martin" had embezzled more than $22,000 to pay for pornography he did not want to show up on his credit card.

Wait a moment! What tipped off the Feds that there was a fraud?

The charges were submitted for reimbursement from Medicare!

Sexual deviance 2:

A 30-year veteran attorney reportedly stole over $77,000 from his firm. A senior partner learned "Scott" was downloading porn on his company computer and sending explicit emails to his lover. "Scott" admitted his guilt and wrote a check for $77,000 to pay back what he had stolen.

Wait, he wrote a check from his own account to cover the $77,000?

Four months later, the firm learned "Scott" had actually embezzled nearly $300,000 from six of the firm's clients and the firm through overbilling!

Power deviance is far more alarming. In fact, Hubbs' research revealed that those who engaged in power deviance in the workplace were involved in much more serious schemes and crimes. The following list is chilling:

- Advance fee scams;
- Arson;
- Extortion;
- Grand larceny;
- Forgery; and
- Identity theft.

And worse:

- Stalking;
- Felony robbery;
- Conspiracy;
- Mortgage fraud;
- Tax evasion; and
- Murder!

F. Caveat 1

There are several things we need to keep in mind while reviewing this intriguing information. One issue to consider is that most frauds do not reach the newspapers. In fact, most fraud perpetrators are never criminally charged. Would a payroll fraud or any other fraud scheme at your organization be newsworthy? Would it have to involve a well-known organization and a large amount of money? Would it have to be related to a government contract or disaster relief?

Perhaps the fact that a public figure or person in the public trust is involved makes the story newsworthy, especially when deviant behavior is added to the tale. The mere fact that deviant behavior is involved may skew the results. Hubbs freely admits in his article that more research needs to be done to test the correlation of deviant behavior and fraud. I continued to search for updated studies with some luck. I found older studies and academic papers on the phenomenon. You can search "deviant behavior and fraud." It will not hurt to also use the British spelling of "behaviour" since many published papers and articles are from the United Kingdom or former British colonial countries.

While we have just made an argument to suggest that 126 news stories in three months may be too many because of the deviant behavior, there is a flipside. Consider that most fraud investigators are not concerned with finding deviant behavior. The investigator is called in to review a set of financial documents to determine if fraud occurred. The investigator is not going to human resources to see if there have been complaints lodged against the suspect regarding deviant behavior in the workplace. Even if

the investigator does ask human resources to provide information, human resources will most likely deny the request. Similarly, human resources professionals receiving a complaint about workplace deviant behavior may not think to seek a fraud investigation. They do not see a connection. (They may even call it a "fishing expedition.") This means that the 126 stories Hubbs found may be fewer in number than what may have been reportable in the same timeframe.

G. First-hand instance

In addition to being a certified fraud examiner (CFE), Hubbs is a professional in human resources (PHR). He was asked to wear his PHR hat and investigate a case of alleged bullying and retaliation. Hubbs' investigation revealed that the charges leveled were false and the accuser was, in fact, downloading inappropriate material (sexual deviation) at work! So, Hubbs changed hats. He put on his CFE hat and started looking at the false accuser's expense reports. It did not take long for Hubbs to realize there were several fraudulent items in the reports. Deeper examination revealed the false accuser (power deviation) had stolen some $20,000 over two years with phony business expenses. Perhaps the key is that the perpetrator engaged in both sexual and power deviance to attempt to cover their money deviance.

Imagine if the investigation stopped when it was revealed that the accuser had trumped up the bullying and retaliation charges? These charges were false, at worst, or maybe overblown by human emotional response. This probably happens every day at some company where an investigation indicates there is no merit to the charges, and they are dropped. All sides agreed "to let it go" and move on (unless someone is a frequent complainer, in which case they may be terminated). Yet by now Hubbs was developing a theory and felt this drama was covering something else.[3]

H. Caveat 2

As mentioned above, there are times when the fraud triangle does not quite fit the scenario because the perpetrator has some desire or need emanating from some psychopathic or sociopathic issue. John D. Gill, J.D., CFE writes in *Fraud Magazine* that certain schemers, such as Bernard Madoff, have certain psychopathic traits that permit them to steal not only from people they do not know but also from friends and family![4] Gill goes on to state that there may be "a possible subset of psychopaths [who] often move from business to business just for the thrill of pulling off fraud crimes."[5] The thrust of Gill's article is that often we bring the fraud triangle into a courtroom to prove fraud. Gill advises that we stick to the facts of what happened, as he writes, "Actions speak louder than words."[6]

Another author, a private investigator from Nashville, Tennessee, noticed Hubbs' article, and wrote:

> Deviance is relative, Hubbs admits. "What is deviant behavior today might not be deviant behavior 20 years from now." And he says that most of us do things every day that might deviate from laws, norms, or workplace policies. But a good investigator with strong instincts about human behavior and motivations, he asserts, might be able to sniff out financial malfeasance by focusing on patterns of behavior that reveal an employee's or contractor's ... proclivities. If a person tends towards risky behaviors, like downloading thousands of pornographic images onto his work computer or texting inappropriate messages or images to co-workers, he might also take risks in other ways, like fudging expenses or rigging bids.[7]

---

3 Hubbs, Ryan C. (CFE, CIA, PHR, CCSA) "Find Deviant Behaviors, Find Fraud?" *Fraud Magazine* Vol. 27 No. 2 March/April 2012: 18-24.

4 Gill, John D. (J.D., CFE) "The Fraud Triangle on Trial," *Fraud Magazine* Vol. 32 No. 5 September/October 2017 pp. 18-23.

5 Ibid. p. 21.

6 Ibid. p. 23.

7 Humphreys, H. (January 25, 2016). All Fraud Investigations Lead to...Porn? Retrieved January 6, 2018, from http://pursuitmag.com/all-fraud-investigations-lead-to-porn/.

What do “most of us do…every day that might deviate from laws, norms, or workplace policies”? The author of the above article did not list them. However, it is easy to find a few. Consider a driver bending the rules of the road – either by going above the posted speed limit, by speeding up to make the light when it turns amber, or even by cutting someone off. Do you know anyone who has fooled around on their spouse? There was a time when affairs were such scandals, and no one spoke of them. Is that true today?

III. 2022 Report to the Nations

Fraud prevention and detection may have always been aware of red flags – such as someone spending above their known means. It has taken time, though, for Hubbs’ “human resources-related red flags” to take hold. When your author spoke to folks in HR, they bristled at sharing such information. But in the report, we find interesting results.

The data showed that only 50 percent of fraud perpetrators experienced “negative HR-related issues prior to or during their frauds.” Keep in mind that not all fraud schemes are detected or reported – even in the report. However, for those who had issues, those most common were:[8]

Fear of job loss	16%
Poor performance evaluations	15%
Denied raise or promotion	12%
Cut in benefits	7%
Pay cut	6%
Actual job loss	6%
Involuntary cut in hours	4%
Demotion	4%
Other	2%

These add to 72 percent, and it is possible that some fraud schemers had more than one HR issue. Notice that “sexual deviance” does not appear specifically unless it is included in “Other.” The report does not elaborate. Fear of job loss was second in 2020, but the pandemic certainly scared a lot of people, even if that fear did not rise to the level of committing a fraud. We ought to consider, as well, that *not* having folks in the office may have thwarted opportunity for some potential schemes. People working from home may also have created a need for additional controls, not the least of which may have been system monitoring. This could really dampen the desire to try a scheme. Conversely, a certain anonymity from being at home rather than at an office workstation may have damaged camaraderie. This form of social distancing may have prompted someone to act, sensing “no one is watching.” The ACFE’s 2022 report found that operational process changes were ***not a factor*** in 60 percent of frauds. Similarly, the shift to remote work was ***not a factor*** in 62 percent of fraud schemes.[9]

---

8 Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*. Association of Certified Fraud Examiners, p. 59, Fig. 46.

9 Ibid. p. 40.

IV. Summary

There is no doubt that our colleagues in the HR area will be loath to provide us with what they consider to be confidential information about an employee if we inquire because we are conducting a fraud investigation regarding someone. They may be even more reluctant should we make a request to know who has had complaints lodged against them, the nature of those complaints, and what the investigation revealed, as there may be fraud involved even though we may not have a lead. When we tell the HR staff that we want to know because it is possible this person (or these people) may be committing fraud based on one article in a fraud prevention magazine, they may be even more skeptical. This one article is, perhaps, insufficient evidence to alter the basic instincts of the HR staff to believe there should not be a larger investigation encompassing fraud just because someone is found to be an abusive manager or is reprimanded for misuse of company assets, such as using their computer to view or store inappropriate material. Think of the phrase, “Let’s not make a mountain out of a mole hill.”

One wonders how the employee Hubbs investigated for possible fraud after allegations of harassment were found to be untrue might have felt if he or she discovered that Hubbs launched a fraud investigation on a hunch. The best course of action here may be to reach out to corporate counsel regarding whether such an investigation could be performed based solely on a complaint to HR.

Yet, with all that said, it is important for us to know that fraudsters may be able to hide their scam but are unable to hide their basic human flaws.

Historic Schemes

Historic Schemes

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Understand some of the biggest fraud schemes perpetrated;
- Understand that employees are motivated in many ways; and
- Realize that trust is earned and maintained over time, and we should never assume everyone is completely honest.

I. Background

In the late 20th and very early 21st centuries, American investment markets were rocked by scandals. Several large companies such as Enron, MCI/WorldCom, and Adelphia were caught cooking the books. They committed financial statement fraud to make their company appear healthier and wealthier than they actually were, or they used the company as a personal bank account. Investors lost billions of dollars. Employees at Enron, for example, lost their entire retirement savings because the retirement accounts were invested exclusively in Enron stock. The impact of the company's collapse in the Houston, Texas area was instantaneous and deep.

As a result, the United States Congress passed the Sarbanes-Oxley Act of 2002 (SOX). Signed into law by President George W. Bush on July 30, 2002, just 15 days after it was introduced on the floor of the Senate and having passed the House of Representatives in April[1], the legislation changed the way publicly traded companies would do business. Any company, whether foreign or domestic, that traded equity or debt on a United States market, would be subject to the law. Management had to assess whether the internal controls over financial reporting they had in place were actually present and operating effectively. In addition, the external auditors would render two additional opinions related to the financial statements. One opinion would attest that management did perform their assessment of their internal controls over financial reporting. The other opinion would state whether the auditors believed the controls were in place and were designed and operating effectively.

In the intervening years since then and now, the requirement for the two extra opinions has been modified. Auditors still assess whether the controls are in place and operating effectively. Other modifications have been made to SOX that are beyond the need of discussion in this course. Even with all the emphasis on having strong internal controls over financial reporting, fraud schemes take place. Some of the biggest or more outrageous are discussed below.

[1] More remarkable was the fact that the bill had to also pass through a conference committee and pass both the House and Senate before going to the president for his signature in that 15-day span!

Meanwhile, the Federal Bureau of Investigation (FBI) maintains a website listing common fraud schemes. The address is https://www.fbi.gov/scams-and-safety/common-fraud-schemes. The site is based on tips the FBI receives and investigates. Some of these schemes ought not to be a surprise. On the list are telemarketing schemes. The FBI says that there are warning signs of this fraud when the caller says things such as:

- "You must act 'now,' or the offer won't be good."
- "You've won a ['free' gift, vacation, or prize]." Yet you must pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." The FBI says that you hear this very quickly before you have a chance to consider the offer.
- Remember, if anyone tells you that they need to access your computer, it is a SCAM!

In addition, the FBI says to be wary of any caller who says you need not check out the company or the offer with anyone, such as your lawyer, accountant, the Better Business Bureau, or any of the other consumer protection agencies.

The FBI describes the so-called "Nigerian Letter" or "419" fraud. In this case, you receive an email from some "Nigerian official" who is attempting to get money out of Nigeria illegally, and they are offering you the opportunity to share in millions of dollars of profit. This scheme targets someone "who has demonstrated a 'propensity for larceny' by responding to the invitation," the FBI writes on its site. In addition, the FBI states that most law-abiding citizens find this a laughable scheme, yet millions are lost each year because there are enough people willing to send money to cover "taxes, bribes to [Nigerian] government officials, and legal fees."

Identity theft is still a major problem, and there is a separate site just for it! Go to the Federal Trade Commission's website at https://www.identitytheft.gov/ to learn more.

You can't make this up:

In the early fall of 2017, I was visiting friends. One friend, Mary, told me that she had been a victim of identity theft because a guy had somehow managed to add his name to one of her credit cards. Fortunately for Mary, the card was through a bank Mary used. Their fraud prevention department contacted her and asked if she had intended to add this man to her account. Mary said that she did not, and the bank and Mary filed a complaint with the local police.

A detective from that department brought the man in for questioning and asked the man to open his wallet. There police discovered that this man had opened another credit card using Mary's information at a second bank. Mary did not use this bank. Mary contacted the fraud prevention department at this bank. The bank representative was stunned to learn that Mary knew who the man was, his address, and, by the way, that the man was already under arrest. Mary asked the bank's representative if she could be told about the application. The bank representative was happy to share the application information.

This is where the story veers into the bizarre. According to what Mary was told, the man said that Mary earned $120,000 a year as a Walmart greeter! Mary asked the bank representative, "And that got through?" The bank's fraud prevention representative had to admit that it did.

QUESTION: Have you taken the preventative step to block unsolicited credit offers from being mailed to you? If not, you may want to do that by visiting www.optoutprescreen.com to opt out of receiving credit offers. These offers could be stolen from your mail or even your trash!

Advance fee schemes mean the victim pays money to someone in anticipation of receiving something of greater value – such as a loan, contract, investment, or gift – and then receives little or nothing in return.

The Bureau reports that the variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or many other "opportunities." Clever con artists then offer to find financing arrangements for clients who pay a "finder's fee" in advance, requiring their clients to sign contracts agreeing to pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the "finder" according to the contract. **Warning**: Such agreements may be legal unless it can be shown that the "finder" never had the intention or the ability to provide financing for the victims.

Tips from the FBI to avoid such schemes:

- If the offer of an "opportunity" appears too good to be true, it probably is. Follow common business practice; that is, legitimate business is rarely conducted in cash on a street corner.
- Know who you are dealing with. If you have not heard of a person or company that you intend to do business with, learn more about them. Depending on the amount of money that you plan on spending, you may want to visit the business location, check with the Better Business Bureau, or consult with your bank, an attorney, or the police.
- Make sure you fully understand any business agreement that you enter into. If the terms are complex, have them reviewed by a competent attorney.
- Be wary of businesses that operate out of post office boxes or mail drops and do not have a street address. Be suspicious when dealing with people who do not have a direct telephone line and who are never in when you call but always return your call later.
- Be wary of business deals that require you to sign nondisclosure or non-circumvention agreements that are designed to prevent you from independently verifying the bona fides of the people with whom you intend to do business. Con artists often use non-circumvention agreements to threaten their victims with civil suits if they report their losses to law enforcement.

Health care or health insurance fraud remains on the list. The schemes vary since the victims could include an insurance company charged for services or tests that were never performed or patients who received "free" products in exchange for providing their Medicare number. It is no surprise, then, that the FBI has a site dedicated to health care fraud at https://www.fbi.gov/scams-and-safety/common-fraud-schemes/health-care-fraud-or-health-insurance-fraud. This area of fraud has been around since health insurance began, maybe even before then. Do you really know what tests are being run when a few vials of blood are drawn? Do you ever check the doctor's order and keep a copy so you can check results against the list of tests that were ordered? If you had a vitamin D level check, you ought to find out what your level was. If the test was not ordered, then a result ought not to appear on your results. Do you review your explanation of benefits (EOB) when your insurance company advises you of a claim?

Another common scheme the FBI discusses on its site is what is referred to as "Redemption, Strawman, or Bond Fraud." The scenario is simple. The fraudster contacts the potential victim and says that the United States government, or specifically the Treasury Department, controls bank accounts for all U.S. citizens. These "U.S. Treasury Direct Accounts" can be accessed by anyone who submits the right paperwork. The scam relies on discredited legal theories and may refer to the scheme as "Redemption,"

“Strawman,” or “Acceptance for Value.” The fraudster promises trainers and websites that charge very large fees for “kits” that teach the potential victim how to perpetrate the scheme. The fraudster implies tremendous success by others who have managed to pay off debt and purchase big ticket items such as homes. Naturally, failure follows the victim, who is told that they did not file paperwork in a timely manner or did so in the wrong order. The inclusion of phony documents such as “bills of exchange,” “indemnity bonds,” “offset bonds,” “sight drafts,” or “comptroller’s warrants” make the scheme seem legitimate. Still not to be out done, misused legitimate forms such as Forms 1099, 1099-OID, “Original Issue Discount,” and 8300, “Report of Cash Payments over $10,000 Received in a Trade or Business” are added to the mix. For more information on these go to https://www.fbi.gov/scams-and-safety/common-fraud-schemes/redemption-strawman-bond-fraud.

Since we are here, let us add what the Internal Revenue Service refers to as the “Dirty Dozen” Tax Scams for 2019, released March 20, 2019. They are in the order the IRS lists them: phishing; phone scams by criminals impersonating IRS agents; identity theft; return preparer fraud in stealing refunds or committing identity theft; inflated refund claims; falsifying income to claim credits; falsely padding deductions on returns; fake charities; excessive claims for business credits; offshore tax avoidance; frivolous tax arguments; and abusive tax shelters. For more information on each of these go to https://www.irs.gov/newsroom/irs-concludes-dirty-dozen-list-of-tax-scams-for-2019-agency-encourages-taxpayers-to-remain-vigilant-year-round.

There are some other investment-related fraud schemes the FBI has run into frequently. Letters of credit (LOCs) are legitimate means of financing, but they are never sold or offered as an investment. Generally, LOCs are used “to ensure payment for goods shipped in connection with international trade.” The confidence artist promises huge returns on investment of an LOC or “bank guarantee” as the investment. As with any fraud scheme, if it sounds too good to be true, it probably is too good to be true and is not real. Con artists rely on an overall lack of understanding of investments and financial markets to lure the victim. Always independently verify investment opportunities before investing.

This scheme leads right into the next investment-related fraud – prime bank note fraud. This scheme is perpetrated on an international scale. The fraudster claims access to “bank guarantees,” as referenced above, offering huge returns! Moreover, these alleged investments have the backing of the world’s largest banks. Due diligence is key to avoiding the trap.

Ponzi schemes remain in the mix, as well. The FBI has websites dedicated to Bernie Madoff and R. Allen Stanford. But there are two other sites the FBI set up, one for ATMs and the other for wholesale grocery distribution as discussed below.

Back in 2009, the FBI revealed on their ATM fraud site that Vance Moore II and Walter Netschi promised investors large returns investing in automated teller machines (ATMs) that would be located in high-traffic retail locations around the United States. The victim would receive between 20 and 24 percent return on their investment! It did not take long for the scam to unravel. Early investors were pleased as some 4,000 ATMs were allegedly purchased and placed in service. In fact, less than 10 percent actually existed. According to the FBI, $80 million was involved when the case closed. See http://www.fbi.gov/news/stories/2009/october/ponzi_100209 for complete details.

About one year later, in 2010, the FBI says they shut down a fraudster who was living the high life in Miami, Florida. According to the FBI's site at http://www.fbi.gov/news/stories/2010/may/ponzi_050310, Nevin Shapiro had a $5 million mansion, a million-dollar yacht, leased Mercedes-Benz cars, and had floor seats at Miami Heat NBA games costing a whopping $400,000. The FBI states that Shapiro convinced investors by providing fake documents that included financial statements of a wholesale grocery distribution business, personal and business tax returns (fraudulent!), faked invoices, and faked promissory notes reflecting the victim's investment amount. This, too, ended up with some $80 million "invested," and the scheme fell in on itself. The FBI defines a Ponzi scheme on the Common Fraud Schemes page as, "[A] promise [of] high financial returns or dividends not available through traditional investments. Instead of investing the funds of victims, however, the con artist pays 'dividends' to initial investors using the funds of subsequent investors."

Closely tied to Ponzi schemes are pyramid schemes. The difference is that in the case of the former, the schemer reaps all the rewards. In the case of the latter, investors are encouraged to find their own investors who fund the fraud up the chain. Participants may withdraw, especially those who were early into the scheme, and may have made money. The pyramid collapses on itself as others attempt to cash out or cut their losses. It ought to be mentioned here, too, that there are businesses set up as what is referred to as either "layered marketing" or "multi-level marketing." Folks are asked to become a distributor, usually having to buy their initial inventory and marketing supplies. They are also encouraged to find new distributors. These schemes tend to start off as help-wanted advertisements, followed by an interview. When someone says, "Congratulations, you have the job! All I need from you is $1,000 to get you started," beware!

II. Background 2.0

Let us discuss the top methods of payment in fraud schemes as reported by EKN and Radial Research Partner in their white paper "Trends in e-commerce & digital fraud: Mitigating the risk." Perhaps it is not surprising that the number one method to pay for something fraudulently is through phishing. My simple rule: I do not open an email I do not recognize, and I never open a link in an email I was not expecting. If it comes from my friend Bob, I am going to call Bob to see if he sent it before opening it.

The FBI mentions identity theft, and EKN/Radial mention it too. According to EKN/Radial, hackers simply penetrate firewalls on old security systems or hijack login credentials on a public Wi-Fi. Many folks will gladly take free Wi-Fi at a store or restaurant rather than go through their phone's data plan. Fraudsters love this. The best practice is to wait until you get home and use your own Wi-Fi or invest in a personal mobile Wi-Fi. (By the way, I did this while traveling overseas, and it worked great! I could even use my phone's navigation applications!)

A corollary to personal identity theft is that of merchant identity fraud. In these cases, a fraudster sets up what appears to be a legitimate business. The perpetrator uses stolen credit card information to charge those cards fraudulently. By the time the victim card holders see the charges, the site is gone, along with the money. It is the facilitator who bears the liability. To help yourself and everyone else in the e-commerce chain, log into your credit card and bank accounts several times a week.

Advance fee and wire transfer scams, as mentioned by the FBI, in some cases target credit card users and e-commerce store owners. Beware of anyone saying they need money now and will repay it later.

Pagejacking is a rather pernicious ploy whereby a very popular page is hijacked in full or in part to divert unsuspecting users to a different website. On this second site may lurk malware that hackers can utilize to gain access to your system. If you are a leader in your firm or company, it may be wise to inquire how secure your website is from hijackers and how secure your system is when employees surf the web.

With this background, let us turn our attention to some of the biggest, most outrageous recent fraud schemes in the news.

III. Bold and brazen

A. Big fish spawn

One of the biggest frauds perpetrated in recent years was a Ponzi scheme by New York investment advisor Bernard Madoff. You may recall that Madoff had run the scheme for many years. Well-known investors flocked to him to deposit money in accounts Madoff claimed would earn well beyond what other investments were yielding at the time. His story is well-known. But there is another fraud many people do not know about that is even bigger.

R. Allen Stanford also ran a Ponzi scheme using bogus certificates of deposit in an Antiguan bank he owned. Stanford was convicted in March 2012, and he was ordered to relinquish 29 bank accounts in his name that totaled around $330 million. He was sentenced on June 12, 2012, to serve 110 years in prison for his fraud costing $7 billion.

Madoff and Stanford were big news at the time their stories broke. Media covered these fascinating and heartbreaking stories. Very wealthy and intelligent people were tricked into a classic scheme. No doubt this was the death of the Ponzi scheme. No one, especially investors in New York, would ever fall for an investment that seemed too good to be true. Right?

Wrong. In late January 2017, two men were charged in a Ponzi scheme that, if true, perhaps has Madoff and Stanford wondering, “They actually tried this!?” It is an alleged case of real life imitating art, in a sense.

Remember Mel Brooks’ classic movie, “The Producers,” which became a smash hit on Broadway decades later? The premise was that two guys would produce a colossal flop of a Broadway show after getting dozens of wealthy widows to invest money for a fifty-percent stake in the show. Naturally, the show turns out to be a huge success, leaving the main characters in jail. According to a *Fox News* report, two men were arrested and charged in New York on January 27, 2017, for running a Ponzi scheme not far from what Brooks imagined. The difference was they allegedly did not invest in the show; the alleged victims invested in large blocks of the tickets to shows like “Hamilton” and Adele concerts (both are specifically identified in the criminal complaint), which would be resold at a profit.

Fox News reported, according to authorities, Joseph Meli, 42, of Manhattan and Steven Simmons, 48, of Wilton, Connecticut, allegedly enticed wealthy investors in 13 states into investing a total of $81 million. The Security and Exchange Commission (SEC) further alleged that $51 million was distributed to early investors seeking their return on investment or for personal expenses of the alleged co-conspirators.

The story quotes William F. Sweeney, Jr., the FBI's Special Agent in charge of the New York office, stating the bitter truth for those who seek to swindle using this form of scheme. He said, "When fraudsters think they're going to get away with scheming investors out of money, they tend to forget that at some point the money will run out. It's the way a Ponzi scheme ends." The article indicates this is what happened – investors wanted their money.

The criminal complaint alleges that the scheme ran from November 2015 until the day the two men were arrested.[2] Not to be outdone, *Bloomberg* reported another man, who had allegedly bilked his high school students of cash 14 years earlier, also entered the realm of fake tickets. That story can be found at https://www.bloomberg.com/news/articles/2017-05-31/ticket-brokerage-ceo-charged-over-alleged-ponzi-scheme.

Question to ponder:

Why do you believe very wealthy, intelligent people can invest thousands of dollars in a scheme, even after tremendous attention has been placed on major frauds?

B. The party girl

Kinde Durkee was the California Democratic Party's treasurer for many years. In early 2012 it was alleged she stole over $7 million in a 10-year span from over 50 clients. California prosecutors further alleged at the time that Durkee used campaign funds for Senator Dianne Feinstein to pay a $23,000 bill on Durkee's American Express charge card. But Durkee was not finished stealing from Senator Feinstein. The prosecutors went on to allege that Durkee stole another $4.7 million, which Senator Feinstein had to replenish from her personal funds.[3]

In time, Durkee was convicted and sentenced to serve eight years in prison and repay $10.5 million taken from the Democratic Party campaign till. However, one California investigator said the money had been "frittered away." There was less than $100,000 available to repay what had been stolen.[4]

If you are getting the impression that the 1980s' mantra of "trust, but verify" has validity when it comes to financial dealings, then the next story of a municipal employee's gallop to fraud infamy will certainly reinforce the point.

C. The horse trader

Rita A. Crundwell had been the Comptroller for the City of Dixon, Illinois since the early 1980s. One can only imagine the shock of hearing that after nearly 30 years of service, the Federal Bureau of Investigation (FBI) was charging Crundwell with embezzling millions of dollars starting in 2006! The FBI alleged she stole the city's funds to support her championship horse breeding ranch and a lavish lifestyle she seemed to convince others went with the successful ranch.

---

2 FoxNews.com (January 28, 2017). "2 men allegedly raised $81M in 'Hamilton' Ponzi scheme."

3 FoxNews.com (March 28, 2012). "Prosecutors: Democratic campaign treasurer embezzled at least $7 million from multiple clients."

4 McGreevy, Patrick. (2014, January 14). "Kinde Durkee short in restitution for $10.5-million theft." *Los Angeles Times*, online.

In court documents filed, the FBI stated Crundwell pilfered $3.2 million from the fall of 2011 until the date of her arrest on April 17, 2012. Equally stunning to those who knew her is what FBI agents seized from Crundwell's property. The list included a 2009 Liberty Coach motor home valued at $2.1 million and a 2009 Kenworth T800 tractor truck to haul her horse trailers pegged at $146,800. Other trucks and trailers valued over $455,000 were seized. In addition, Crundwell had allegedly purchased jewelry totaling $339,000, and there were two bank accounts.

The most dizzying facet of the allegations was found in the final tally. Initially thought to total $30 million, the FBI eventually alleged that Crundwell stole $53 million dollars over the years from a small city with an annual budget of just $20 million. Furthermore, agents seemed to trace only $450,000 of the funds stolen to Crundwell's horse farm. Thus, it begs the obvious question: how was this fraud scheme missed?

There were many factors that conspired to cover the deception. The fraud was ultimately discovered when a staffer filling in for vacation help discovered what turned out to be a secret bank account. It was quickly determined that the city's longtime comptroller had far too broad power and access. There was a lack of segregation of duties. Crundwell could get a check produced from start to finish. Internal controls were exceedingly weak or nonexistent, and there was another opportunity Crundwell could seize upon to cover her tracks. The state of Illinois was behind in its payments to municipalities; therefore, Dixon's budget problems could easily be blamed on those in the state capitol, Springfield. No one suspected that the problem might be caused by fraud.

If the state's problems were not enough, Crundwell had another advantage. People attributed her lavish lifestyle to the success of her championship horse farm; she had trophies and ribbons, the mark of success. Clearly, it seemed, there was good money in the horse breeding business. Even so, no one ever asked why someone with such success and available money would want to keep a full-time job that paid $80,000 a year.[5]

D. Source over and out

Many businesses – both large and small – outsource their payroll processing. Payroll is very complex, and having a company ensure that all payments are made to employees and the proper tax authorities in a timely manner can relieve stress. There are many payroll service providers out there. But with anything else, buyer beware. Consider this, sadly, not all too rare occurrence in Los Angeles, California.

Started by Gene Moroz, LA Payroll had been in business for more than 10 years, with an office on posh Wiltshire Boulevard. Over 150 client companies used LA Payroll to process their payrolls. There were never any problems, that is, until late December 2013. LA Payroll staff received dozens of notices from the Internal Revenue Service as well as taxing authorities in California. It seemed the clients' tax payments were not being made. Just before the notices arrived, the current owner of LA Payroll, Tovmas Grigoryan, announced he was going to leave for a Palm Springs vacation.

---

[5] FoxNews.com (April 29, 2012). "Longtime city official accused of staggering $30M theft from tiny Illinois city." *Associated Press*.

Clients were stunned. They were shocked their money – upwards of $7 million in total – was gone, and the 56-year-old Grigoryan was the owner (his involvement in the company was never revealed) with sole control over the clients' impound accounts. Moroz told the *Los Angeles Times* that he sold LA Payroll in 2011 to Dmitri Paiu. Moroz stayed on to consult for a time, and in 2012, Paiu introduced Moroz to Grigoryan, who Paiu said was his new partner. Moroz's consulting ended. He never suspected there was anything wrong with either fellow.

Days before Christmas, staff at LA Payroll contacted clients to inform them that they had outstanding tax liabilities. The clients were all responsible for making the tax payments, plus interest and penalties. While lawsuits have been filed, and charges pressed through law enforcement, there is little hope that the money will ever be recovered. Authorities have no idea where Grigoryan is. He could be in Russia, Armenia, or anywhere else.[6]

IV. Final thoughts

If you use a payroll service, it is highly advisable that you also maintain a watch on your various tax accounts with authorities. You ought to be able to access your account with the IRS, as well as with the various states' tax authorities. Any payroll service provider who will not welcome your oversight ought to give you serious pause.

There are many people who have second sources of income. The most prevalent second income source is from a spouse or live-in partner. Some people may even have a second job, a hobby or a small business, such as a horse breeding farm, that provides extra cash. If you know that someone has an apparent second source of income, such as Rita Crundwell above, and want to learn more about that source, it can be easily determined. The internet is full of sites for all endeavors that will explain what the expected income for any job is. I was able to determine, based on reviewing several sites, that I could earn – at best – $45,000 a year as a singer if I work every week. As for horse breeding, it seems folks do it for the love of the beautiful animal alone.

Reality check 2:

> Patricia Hampton of North Wind Arabians wrote on the Breeders Corner site, "Raising horses is not a get rich quick business, and in most cases, it is not a get rich slowly business either… ."

What can we look forward to in 2018 and beyond? Bots. Bots are internet robots. You may hear them referred to as web bots, spiders, or something else. In essence, bots can be useful. Some companies are seeking to use bots to perform routine journal entries. The bot can run depreciation for a month, create a journal entry, and even post it. Why use a valuable person's time doing that when that person can be performing work where a human's insight and intuition are more valuable? But you know there is a dark side to this force.

According to the U.K. online publication, *Independent*, we can look forward to bots trying to rip us off!

---

6 Christensen, K. (February 10, 2014). "A payroll company leaves its clients in the lurch." *Los Angeles Times*.

See below for some excerpts from the article, “Fraudulent scams expected to rocket in 2018; Robots, ransomware and rip-offs…how criminals are getting smarter.” The most concerning part of the coming storm is the ability of online fraudsters to target their victims. Phishing will be far more sophisticated. Emails will appear far more authentic. Could being hacked become as much a given as getting a ding on our car simply because we park our car in a public lot?

> …Dave Palmer, director of technology at Darktrace, says: ‘In 2018, we will start to see the emergence of threat-actors harnessing AI technology to launch sophisticated, automated campaigns.
>
> “Imagine a piece of malware that can train itself on how your writing style differs depending on who you are contacting, and leverages this nuanced understanding to send tailored, contextually relevant messages to your contacts.
>
> “These phishing messages will be so realistic that the target will fall for them, downloading malicious attachments or following dangerous links. Such advances in AI will take us to the next stage in defenders versus attackers, and we need to be ready.”
>
> …[Some] commentators say there will be more personalised attacks, with larger corresponding demands. Graeme Newman, chief innovation officer at CFC Underwriting, says: “We continue to see ransomware grow as a threat. Last year, ransomware accounted for almost 25 percent of all our cyber claims (up from 10 percent a year ago). Next year, however, we believe this will morph towards more targeted attacks with higher ransom demands.”
>
> Rich Smith, Duo Labs director at Duo Security, comments: “Watch out for fraudsters purporting to be from the government or offering to protect you against something the government is supposedly doing. Scams often exploit someone’s emotions rather than rationale, tugging at people’s heartstrings or tempting them with salacious material. The ‘fake news’ epidemic will get worse before it gets better, so don’t be in a hurry to respond to sensational pronouncements of any kind.”
>
> [There was] a real surge [in 2017] in the number of email intercept fraud cases, where criminals hacked into accounts and emailed customers pretending to be a business but providing them with the wrong account information. In a number of these cases the banks will not help as the victim proactively made the transfer themselves. Newman believes this is going to develop into an even larger problem in 2018 and that the criminals are becoming even more convincing.
>
> He says: “Email hacking due to increased use of web-based mail applications and a lack of basic security controls amongst SMEs will lead to a huge increase in social engineering scams. By combining information found in inboxes with social media postings, cyber criminals will craft increasingly convincing emails to con unwitting recipients into transferring funds directly into the criminals’ bank accounts. We expect this form of scam to grow from 10 percent of our total claims last year to be our number one source of losses.”
>
> Joseph Carson, chief security scientist at Thycotic, says: “Digital insider trading and stealing crypto currencies will continue to be major problems throughout 2018, which could see both economic disruption or the rise and fall of Bitcoin. Where internet scams and fraud rise so will fake news and political disruption.” [7]

The Federal Trade Commission has information at www.ftc.gov under “cybersecurity.”

---

[7] Hannah, F. (2017, December 29). “Fraudulent scams expected to rocket in 2018.” Retrieved January 10, 2018, from http://www.independent.co.uk/money/spend-save/scams-2018-fraud-robots-ransomware-rip-off-bank-accounts-identity-a8131236.html?.

Combating Fraud With Controls

Combating Fraud With Controls

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Understand the most important anti-fraud controls, including digital age controls;
- Understand various ways these controls may be incorporated into your organization; and
- Realize that even with these controls, fraud may still occur.

I. Introduction

Internal controls have been in existence since the beginning of accounting. The first recorded balance sheets were found in ancient Egyptian tombs – written on the walls thousands of years ago! Why was accounting and ensuring the balance of the daily bread so important? Since there was business going on, whatever was being traded, bought, and sold had value. There were taxes imposed on the bread, for example. Therefore, the state's accountants had to be sure they were getting the complete inventory of bread baked each day, sold during the day, and left over at the end of the day. These tallies were done every day.

For more information, see "Accounting and Forms of Accountability in Ancient Civilizations: Mesopotamia and Ancient Egypt" by Salvador Carmona, Instituto de Empresa; and Mahmoud Ezzamel, Cardiff Business School - Accounting and Finance Section; December 5, 2005, Instituto de Empresa Business School Working Paper No. WP05-21 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1016353.

You can also visit https://www.wyzant.com/resources/lessons/accounting/introduction, which has an interesting history of accounting.

If internal controls and attention to fine detail in accounting date back to before biblical times, why is it that we must pass laws in the United States, and other nations, insisting upon internal controls? (The Foreign Corrupt Practices Act of 1977 specifically requires internal controls to account for payments to foreign nationals; and, of course, the Sarbanes-Oxley Act of 2002 added a layer of assurance on the existence and effectiveness of internal controls.) We are about to explore internal controls. We are not going to discuss the top controls to combat fraud and go through 10, 25, or 50 controls. Most businesses have these controls already. If you are seeking peace of mind and the ability to check a box and sleep better, then this is not the chapter for you.

We are about to review controls that we likely have in place right now in our organization that were also in place at fraud victim organizations. These controls are likely implemented at most organizations – public, private, large, and small. Regardless of your organization's type (corporation, partnership, and so forth) and size, it is helpful to incorporate the Public Company Accounting Oversight Board's defining purpose to internal controls: "Effective internal control over financial reporting provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes. If one or more material weaknesses exist, the company's internal control over financial reporting cannot be considered effective." [Footnotes omitted.][1]

[1] Audit Standard (AS) 2201: "An Audit of Internal Controls Over Financial Reporting That Is Integrated with An Audit of Financial Statements," par .02. Retrieved from https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx.

II. Anti-fraud controls

A. Foundation

We have been referring to the Association of Certified Fraud Examiners (ACFE) *Occupational Fraud 2022: A Report to the Nations* for many interesting facts about fraud schemes and schemers. The report also provides insight into the most prevalent anti-fraud controls that victim organizations had in place. Let us be very clear what we are saying here: the controls we are about to explore were in place and presumably functioning in the victim organizations. This ought to serve as fair warning for us, as just having all these controls is not a panacea against fraud. Were these controls fully functional, designed, and operating effectively? The report does not tell us. This question will come up a few more times as we review the controls.

The report provides insight for the reader on both a global and a regional scale. For this next table of controls, we will look at the controls in place both globally and in the United States and Canada. In 2022, the U.S. (in first place) had just over 57 percent more fraud cases than the number two region – Sub-Saharan Africa. 675 cases were studied in the U.S. and Canada compared to 429 cases in Sub-Saharan Africa, although 429 was a whopping 42.5 percent increase over the data in the 2020 report.

Table 1
Anti-Fraud Controls: Global[2]

External audit of financial statements	82%
Code of conduct	82%
Internal audit department	77%
Management certification of financial statements	74%
External audit of internal controls over financial reporting	71%
Hotline	70%
Management review	69%
Independent audit committee	67%
Anti-fraud policy	60%
Fraud training for managers/executives	59%
Employee support programs	56%
Dedicated fraud department, function, or team	48%
Formal fraud risk assessments	46%
Proactive data monitoring/analysis	45%
Surprise audits	42%
Job rotation/mandatory vacation	25%
Rewards for whistleblowers	15%

Before moving on to Table 2, you may want to take a moment in reviewing this list of controls in place globally to note which controls surprise you in their placement on the list. For example, are you surprised to find “anti-fraud policy” as far down the list? Perhaps it ought not to come as a surprise. A person who is willing, able, and capable (think of the sides of the fraud triangle) of committing a fraud scheme really does not concern him or herself with violating a policy. Nonetheless, the policy is meant to get everyone to reconsider the act before going through with it.

One control dropped off completely, though we will see it in Table 2. Fraud [prevention] training for employees is not on the list!

---

[2] Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*. Association of Certified Fraud Examiners, p. 34, Fig. 22.

Question to ponder:

Are there controls you think ought to be on this list? How many controls does your organization have in place?

Table 2
Anti-Fraud Controls: United States and Canada[3]

Code of conduct	74%
External audit of financial statements	72%
Employee support programs	66%
Internal audit department	66%
Management certification of financial statements	65%
External audit of internal controls over financial reporting	63%
Hotline	63%
Management review	63%
Independent audit committee	56%
Fraud training for employees	55%
Fraud training for managers/executives	55%
Anti-fraud policy	51%
Proactive data monitoring/analysis	43%
Formal fraud risk assessments	42%
Dedicated fraud department, function, or team	41%
Surprise audits	35%
Job rotation/mandatory vacation	20%
Rewards for whistleblowers	14%

Are you as surprised as I was when I first pondered the meaning of this information? On the upside, some anti-fraud measures listed saw an increase in utilization, both globally and in the U.S./Canada. Conversely, consider that just 74 percent of the United States and Canada companies victimized by fraud had a formal code of ethics and business conduct. (This is down 6 percentage points from the 2020 report.) Certainly, having a written code of ethics and business conduct is not going to prevent fraud – otherwise, the instance of fraud would be much lower. That is, if having a code of ethics and business conduct for an organization was such a wonderful preventative measure, then the percentage of victim organizations employing this control would be very low. That said, it is still very important to have a code of ethics and business conduct to establish a baseline. Management ought to set a stake in the ground that marks the point below which no one shall go. All other policies the organization promulgates stem from this first policy – the code of ethics and business conduct.

B. Controls

Using the data for the United States and Canada in Table 2 above, let us proceed through this list and discuss each control that was in place. Throughout the discussions of each control, you may want to consider whether your organization has the controls in place, as well as how your organization assesses the effectiveness of their design and operation. As you review this list consider the presence (or absence) of management override in the performance of the controls. Even the first on the list, code of ethics and business conduct, can be overridden when it comes to training, refresher training, and especially follow through on consequences with code violations.

[3] Ibid. p. 83, Fig. 84.

1. Code of conduct (ethics)

Channeling my inner cynic, I might suggest that a code of ethics and business conduct may not be worth the paper on which it is printed. Then again, the codes that I have seen in my career are usually printed on very high-grade paper with extensive artwork. What is the key ingredient in the code? The answer is follow-through by upper management! This means that the organization's leadership not only talks about why ethical behavior is important, they demonstrate it every day! It goes even further than that. If someone violates the code of ethics and business conduct in an egregious manner, the consequences up to and even including termination must be evident to as many people as possible.

Sure, there may be small organizations that do not need a formal, highly produced code of ethics and business conduct. Senior leadership is close to everyone every day. Ethical values can be imparted very easily. For larger organizations, formal documentation becomes more important. It is in these larger settings that management cannot simply distribute the code and hope for the best. Ethics must be engrained in all personnel.

This can also mean that there may have to be some lesser amounts of follow-through when the code is violated even in small ways. Let us expand on that statement above. I cannot emphasize enough how vital this follow-through is to demonstrate a true commitment to integrity and ethics. If someone violates the code of ethics and business conduct, then it is critical to the ethics environment that discipline be administered in accordance with organizational policy and procedure. In fact, if the code of ethics and business conduct is company policy number one, then the policy on discipline ought to be policy number two. The failure to initiate discipline will immediately undermine the code of ethics and business conduct and make it worthless. This could be why we see that this control has seemingly failed to live up to its billing in fraud prevention. In my earlier statement, I said that as many people as possible should be aware that the consequences were meted out. If Employee violates the code in an egregious manner and is terminated, and those who remain in the organization know that Employee was terminated for that cause (the exact cause need not and ought not to be revealed), then the 80 percent of folks who can be tempted will have something new to consider.

Take a moment to note your assessment of your organization's code of ethics and business conduct from the viewpoint of how it is reinforced and enforced through management's actions.

Let us also mention right here that hiring ethical people – one of the one in 10 who will never steal – is most important. Gael O'Brien wrote in *Entrepreneur* magazine that the key to finding honest employees is in the interviewing process. Ms. O'Brien was writing in response to the question of how a small company that cannot afford to use personality tests for potential and new hires can weed out dishonest candidates. The answer is that the company ought to use trusted employees in the interview process because they will naturally seek people who have the same traits, such as honesty and integrity. It is very difficult to fake these in an interview.

"When members of the management team interview candidates, make sure they ask candidates about their definition of resilience, how they handled past mistakes (both their own and those of others) and what they feel they can bring to the work environment you are creating. (Bonus points for candidates who already know about and can discuss your organization's values.)"[4] While Ms. O'Brien admits that there is no guaranteed method, once the person is on board, emphasizing the requirement to act ethically and

---

[4] O'Brien, G (October 7, 2014). "The Ethics Coach on the Secret to Hiring Honest Employees." *Entrepreneur.* Retrieved from http://www.entrepreneur.com/article/237320.

responsibly, along with noting the severe consequences for failing to act properly (up to and including termination) will be a more effective deterrent to poor behavior.[5] Do I need to mention to follow through on the consequences? Probably not.

Another helpful article, titled, "Eight Ways to Hire Honest Employees," published in 2012 on eoforless.com, is geared toward reducing exposure in errors and omissions. Fraud is the ultimate "error," and not detecting fraud and stopping the scheme is the ultimate "omission." This article suggests that it is wise to use every tool available to us in finding truly honest people to hire.[6] Eoforless.com suggests eight steps to follow.

First, the author recommends that we write out exactly what we are seeking in a detailed profile with our desired skills, attitudes, and moral values. The author then makes it clear that we ought not to settle for anything less during the interview. If our gut is unsettled with the candidate, move on.

Second, integrate the organization's core value statement into every job posting, whether directly online or through recruiting services. Make a clear statement that you are seeking individuals who share these core beliefs and values. Eoforless.com also says that you ought to state that you will conduct full background checks and drug screenings on all candidates!

Step three is to review all the resumes and weed out the clearly unqualified people. That is simple enough. But the author suggests that we go further during this review and look for what the author calls "ethical red flags." What are these red flags? They suggest things such as "unusual career transitions, decreasing accountabilities, and long, unexplained periods between jobs." In addition, we can "look for job titles and accountabilities that seem out of proportion to the candidate's training and experience." The author also inserts a positive marker to look for that may point to an honest person. That is, those "people who have been entrusted with large projects and budgets and many employees to supervise have shown they are trustworthy."

After we have screened out those who are not qualified and those who have ethical red flags on their resume, the fourth thing to do is invite some candidates for interviews. The author says this is a "manageable number," and only you can determine what is manageable for you. But take into consideration Gael O'Brien's suggestion of using a team to interview candidates. This will mean managing schedules. What will work best for your organization: schedule different candidates on different days, or schedule several on one day? It may depend on the level of the job you are seeking to fill.

Fifth, go old school and have the candidate fill out a job application. Why? The author writes, "Knowing that many people 'fudge' their answers, 'sell' them on the importance of being honest. Say something like, 'We take honesty seriously around here. So please fill out this application, making sure your answers are totally accurate and complete. Also answer all the questions about recent jobs and please include the actual reasons for leaving. We will be checking with prior employers, so again, be truthful."[7] Wow, if that does not get someone's attention that you are taking ethics and integrity seriously, I do not know what else will. I do want to insert a caveat: do not say that you will conduct full background checks or follow up with past employers if you have no intention of doing so. Lying to the candidate about this tells them something about your organization that is the opposite of what you are trying to establish! That is, you

---

5 Ibid.

6 (2012). "Eight Ways to Hire Honest Employees." *EOforless.com.* Retrieved from http://www.eoforless.com/eight-ways-to-hire-honest-employees/.

7 Ibid.

want to be sure to find honest people because ethics and integrity are core values. Think of it the same way you think of online dating. How many stories have you heard about people meeting someone who described themselves one way, but in person they were not even close to what they described? If someone is willing to lie about their height or body type, what else will they lie to you about? If you are willing to fib on background checks, the new employee now knows that the organization is not serious about ethics and integrity.

The article's sixth step in the process is a meeting with the candidate after they have completed the job application. In this meeting, you should review the information on the application, explain the process you are following, and include the "administering [of] an honesty assessment." The author suggests that the meeting not exceed thirty (30) minutes. Eoforless.com lists three honesty assessments and says that one may search the internet for others. You can also contact your HR staff for suggestions. The three suggested lists are:

- Personnel Selection Inventory (PSI) at www.vangent-hcm.com/Solutions/SelectionAssessments/GeneralAssessments1/PSI/;
- The Reid Report Risk Assessment at www.vangent-hcm.com/Solutions/SelectionAssessments/GeneralAssessments1/ReidReportRiskAssessment/; and
- The Veracity Analysis Questionnaire (VAQ) at www.theftstopper.com/solutions/pre-employment-testing/veracity-analysis-questionnaire/.

I would suggest that if you are to take this step, it is important to be consistent with all candidates. Either they all take the test or none of them do. You may even want to consult with general counsel and HR before implementing this step.

Now that we have the test results, we are ready for step seven: to screen out the problematic candidates. But step seven does not end there. The author says that it is time to contact the remaining candidates to schedule more detailed interviews. This is the time to go over prior jobs and the reasons for leaving, as well as getting a sense of what the candidate's job goals are in the future. The author also recommends asking probing questions focused on ethics. Some suggested questions listed are:

- Have you ever observed a work colleague steal? What did you do about it?
- Have you ever had a boss, colleague, or vendor ask you to do something wrong? How did it make you feel? What did you do about it?
- Have you ever done anything yourself at work that bothered your conscience? What was it and how did you respond?

Those are tough questions – suitable for polygraph tests! (Not suggesting those.) The author emphasizes that our goal is to find someone who is not only honest but truly shares our core values. Therefore, at this phase, those on the interview team need to have answered these and any other questions beforehand. This will help gauge how candidates' answers blend with your answers and confirm or conflict with your organization's core values.

Finally, we reach the eighth and final step. The author suggests that now is the time to check references and perform the background and credit checks. In regard to reference checks, which can be tricky, the author recommends trying to get an answer to just one question: is the person eligible for rehire? Be sure to follow up if the answer is "no." For example, some organizations may have a policy that they will not rehire anyone who resigns. (I know it sounds small, but I have run into them.) In addition, the background

check may reveal a criminal conviction, and the credit check may uncover large indebtedness. The article recommends comparing the outstanding debt to the starting salary you are contemplating. If the salary will not cover the debt, then it could be a problem.

Only after all of this does the author suggest making the offer.[8] It is rather Pollyannaish to believe we can, in fact, hire only those who fall in the roughly 10 percent of people who would never commit a scheme against our organization. However, having at least one or two in every area of our organization may help, as their moral compass tends to be inculcated in others around them.

2. External audit of financial statements

It is important to remember that our external auditors are part of an overall fraud prevention process, but they are not a cure for fraud or even the main deterrent. External auditors are the fraud detectors in four percent of the global fraud schemes studied by the ACFE for the 2022 report. This seemingly failed control employed by 72 percent of the U.S. and Canada victim organizations should not mean that we can cease having audits performed on our financial statements. What this most likely means is that a typical fraud scheme is well camouflaged by the perpetrator(s). Lest we forget, the average fraud operates for 12 months before detection! The fraudsters are fooling a lot of people every day! These people are the ones in the best position to prevent or detect fraud.

There is also the inherent risk associated with audits in general. Auditors rely upon a sample of transactions to assess whether an account is properly stated. Auditors are seeking reasonable assurance about the value of the account balance. In addition, many audit firms have an expectation of human error in control activity performance. If the error rate is within the bounds of those expectations, then it stands to reason that auditors might bring it to someone's attention but might otherwise pass on performing any additional procedures. Why? The deadline is fast approaching. They must get the audit fieldwork completed in time for the various layers of review, quality control, and follow-up questions. And we can add that they also have a budget to meet. More time spent on investigation increases the cost.

Perpetrators are skilled at providing phony documentation that looks authentic. As our external auditors are looking at thousands of numbers in a day, it is easy for them to miss that a cab receipt on two different days in two different cities somehow managed to have the same transaction number. Our own internal gatekeepers are in a much better position to notice that if they have time to review documentation and rest during the day. Otherwise, they get number fatigue, too.

Consider and jot down thoughts you have about your external auditors (should you have such audits performed) and/or how you might improve the value of the external audit of financial statements for your organization.

3. Employee support programs

In 12th place globally in 2022, this control is more frequently used in the United States (coming in third in 2022, up from fourth in 2020). The economy impacts businesses and people, and decisions must be made on how best to spend limited resources, such as cash. Still, it seems that having this control in place at the victim organizations was not enough to hamper fraud. This may be due in part because someone determined to commit fraud will do so and will not seek assistance as they do not see a problem with their behavior. Meanwhile, someone who does reach out to the service providers may be far

---

8 Ibid.

less inclined to commit fraud in the first place, be they in the 10 percent who will never steal or the 80 percent of those who can be tempted.

Nearly three-quarters of the U.S./Canada victim organizations used this control to stem what exactly? Is the purpose of the program to ensure people get help with legal issues, health issues, addiction problems, financial concerns, and the like so they can be more productive? Do companies even contemplate that such programs could be used to avert a fraud scheme, or is it simply about maintaining productivity to achieve the numbers? Do employees trust that their support program *is strictly confidential*? Do they fear that their organization will be told, for example, that an employee called about a gambling problem? Do employees believe that their supervisor will be alerted if they contact the support program personnel about financial issues?

It comes down to trust. If one exists, consider your organization's employee support program. How much do you know about the assistance that is available? Do you believe it could be an effective tool against fraud? How could such a program become better at combating fraud? Ask yourself the following questions. If I were having financial difficulty, whether caused by my spouse losing a job or by severe health issues, would I know how to get assistance? Would I trust that the assistance provider would be able to provide the help I need in a confidential manner?

4. Internal audit department

Internal auditors can either be a great resource or an unwelcome distraction. I have worked in organizations where the internal auditors felt it was their duty to find something wrong. To make matters worse, while in one such organization, internal auditors audited certain controls and found *zero* exceptions or deficiencies and still made the official report "needs improvement"! Can you believe that? How could I possibly improve on a series of controls that were designed and operating effectively to the point of having no issues? Yet I was told in no uncertain terms that this internal audit department's mandate was to always find something about which to complain. Like the story of the boy who cried wolf, if an internal audit department always finds fault, I wonder if they lose credibility and risk raising a legitimate red flag only to have it dismissed as just internal audit doing what they always do.

In my mind, the internal audit department ought to be a value-added group within the organization. They act as a new set of eyes that might see something to which the rest of us have become blind. Still, no matter how their role is interpreted, the ACFE 2022 report says that internal audit detects fraud in about 16 percent of the cases. Certainly, this is much better than their external audit counterparts. Is it because they enter the engagement with the desire to uncover problems? Do the auditors and supervisors know the organization well enough to detect a suspicious transaction or expense report better than their external counterparts? Or by limiting their focus to just a few controls, are they able to sample more items, thus casting a wider net and capturing fraud?

Having an internal audit department is worthwhile. Does your organization have an internal audit department? If not, might it be worth considering? In formulating the cost-benefit analysis, consider the median loss for organizations such as yours – industry, size, and others. Then consider the potential for fraud schemes operating simultaneously in your organization. What other factors might management wish to consider in creating an internal audit department?

If your organization has an internal audit department, can you think of ways to increase the value, both real and perceived? Do people in your organization loathe the thought of internal auditors in the office? Can you improve the relationship between the internal audit staff and the finance and accounting staff?

5. Management certification of financial statements

One may believe that if management certifies that the financial statements are free of material misstatements and present fairly the financial condition of the organization, then fraud goes away. One may wish to reassess that belief. When the Sarbanes-Oxley Act of 2002 passed, this control was made law for those companies that were trading debt and/or equity on United States exchanges (a simplified definition). The Congress of the United States believed that fraud would drop, even disappear, if the chief executive and chief financial officers had to sign *personally* for the quality of the financials. Still, all these years after the Act took effect, fraud continues to occur. This means that CEOs and CFOs are signing certifications they believe are true, but someone, somewhere in their organization is making liars out of them. Perhaps liar is too strong a term. Let us say fibbers. Better yet, perhaps the best term for these CEOs and CFOs is misinformed.

Honestly, I do not know how any CEO and CFO of a large organization (one with many locations and thousands of employees) can sleep at night signing such a certification. Consider for a moment if we take at face value reality check 1 in Chapter 1 that 10 percent of our employees will steal every chance they get, then that means 100 people – at a minimum – are stealing in an organization of 1,000 employees. Furthermore, recall that 80 percent of employees may steal if they think they can get away with it. Therefore, these two certifying officers must know that when they are signing the certification letters, there could be dozens, or even hundreds of active fraud schemes underway within the organization.

This control may mean much more to smaller organizations because the certifying officers are closer to the day-to-day activities. They see much more information daily than in larger organizations, information that bubbles up through several layers. The resulting data is sanitized and reduced to a narrower scale to reach the “executive summary” page. How is a CEO and/or CFO going to know if an employee is submitting a phony timesheet? How are the CEO and CFO to know whether 200 widgets were delivered on any given day?

Does your organization have such management certifications of the financial statements? Do you believe that sub-certifications by lower management levels (controller, director of accounting, general ledger accounting manager, etc. following the reporting lines) may improve the value of the CEO and CFO certifications?

Management’s certification apparently is not enough. The Public Company Accounting Oversight Board (PCAOB) re-proposed a standard titled, “Improving the Transparency of Audits: Proposed Amendments to PCAOB Auditing Standards to Provide Disclosure in the Auditor’s Report of Certain Participants in the Audit” on December 4, 2013. The proposed rule was made final with the release of Release No. 2015-008, which you can read at https://pcaobus.org/Rulemaking/Docket029/Release-2015-008.pdf, published on December 15, 2015. The Securities and Exchange Commission (SEC) approved the rule and issued File No. PCAOB 2016-01 on January 29, 2016. You can see this massive 1,951-page document at https://pcaobus.org/Rulemaking/Docket029/SEC19b_4.pdf.pdf. The SEC writes:

> Under the final rules, firms will be required to file a new PCAOB form for each issuer audit, disclosing, among other things: the name of the engagement partner; the name, location, and extent of participation of each other accounting firm participating in the audit whose work constituted at least 5 percent of total audit hours; and the number and aggregate extent of participation of all other accounting firms participating in the audit whose individual participation was less than 5 percent of total audit hours. The information will be filed on Form AP, “Auditor Reporting of Certain Audit Participants,” and will be available in a searchable database on the Board's website.

6. External audit of internal controls over financial reporting

Here is another control tied to the Sarbanes-Oxley Act. Internal controls existed for quite some time before the Act passed in 2002. COSO released an integrated framework for internal control in 1992. Then, in 2004, just as the Sarbanes-Oxley Act was taking hold, COSO released an integrated framework for enterprise risk management (ERM). Control activities were critical to both frameworks, as the activities were put in place to reduce the risk of an organization failing to meet its objectives in one or more of several categories (three in the internal control framework: operations, financial reporting, and compliance; four in ERM, which added strategic objectives). The latest COSO internal control framework modifies the old financial reporting objectives category to a broader term, simply reporting. (And this means *all* reporting the organization performs.)

We are still faced with the same limitation our external auditors face when auditing the financial statements: the volume of numbers and transactions. Auditors can only examine a sample of transactions and related documentation in assessing the effectiveness of internal controls. Fraudsters are usually pretty sharp when it comes to making the transactions look proper. For instance, someone submitting fraudulent expense reports knows where to get fake receipts or how to create them. They may actually start with a legitimate receipt but alter its appearance for submission after the first time. By this I mean, they insert the new “proper” dates and times and amounts but use a software to overwrite the original numbers. This allows them to use the same document again with a new set of numbers, never having to actually incur the expense. How much time can an auditor spend reviewing documents in the hope that they will somehow detect a receipt that looks familiar? After viewing dozens of receipts, will they even remember what they saw two hours earlier? Will they view a large enough sample from the same expense report submitter?

There are other ways fraudulent transactions occur. Consider billing schemes by both the organization and vendors, reports that indicate the wrong amount of product or service received, and journal entries made to alter the financial statements. When we factor in dozens of other tactics used by fraud perpetrators, we must wonder whether there are enough controls. There are not enough controls. In some cases, the more complex and layered the procedure the easier it is to slip something past the gatekeepers.

Make some notes on your internal control system and how it is audited by your external auditors. Have your auditors ever asked about a transaction that they thought might be suspicious? Did you ever follow up on a transaction questioned by auditors even if they gave no indication of their suspicion? Have you ever seen a transaction in a sample and sent it to the auditors to see if they might think it odd, too? How might you get more value from an external audit of your organization’s internal controls?

7. Hotline

Can you believe that this item remains so far down on the list for U.S./Canada victim companies despite the 2022 report again finding that this single control is the most effective weapon in combating fraud, topping the list of detection methods? To fully appreciate the impact a hotline has, let us return to the report.

Table 3
Source of Tips[9]

Employee	55%
Customer	18%
Anonymous	16%
Vendor	10%
Other	5%
Competitor	3%
Shareholder/owner	3%

The 2016 report suggested that fear of backlash for whistleblowing employees may lead to an increase in the number of schemes reported anonymously. The 2018 report expanded on the cause for anonymous tips because, whether internal or external, by stating, "Whistleblowers often have a fear of being identified or retaliated against, which is why it is important that they be able to make reports anonymously where such practice is legally permissible."[10] The 2022 report breaks down the top three parties to whom whistleblowers reported: their direct supervisor in 30 percent of cases, an executive in 15 percent of the reports, and internal audit 12 percent of the time. Reports were also made to a fraud investigation team, "other," the Board or audit committee, and co-workers. The report gives sound advice. First, "not all tips about suspected fraud are reported through a formal reporting mechanism. Some reports are made informally to individuals within the organization." This makes sense. Does your organization have a form to fill out? There may be an "online form" to make a report, but folks "blowing the whistle" are typically reluctant. The report goes on to advise, "Because almost anyone in an organization could potentially receive a report, it is important to provide staff with guidance on how fraud allegations are handled… ."[11]

Curiously, the number of fraud schemes detected via tip – regardless of the source – in the United States and Canada region remains just 32 percent.[12] This may corroborate what was just stated, that people fear some form of retaliation for blowing the whistle. (In fact, I have experience within organizations where it was clear that employees did not trust the anonymity of the ethics hotline.) We also want to understand that not all tips came in via a hotline. Many organizations in the study did not have hotlines.

The 2018 report did not break out the overall impact of those organizations with a hotline and those without, as Table 4 below shows from the prior 2016 report. However, the 2022, 2020, and the 2018 reports make clear that there is still a big difference. For instance, the 2018 report stated that fraud losses were 50 percent less where hotlines were available. Conversely, organizations without a hotline were twice as likely to detect the fraud scheme by accident or by their external auditors.[13] In the 2020 report, median losses were nearly twice as high in organizations without a tip line ($100k to $198k). Just as compelling, having a hotline shaved six months off the median duration of the scheme (from 18 down to 12 months).[14]

Globally, the 2022 report states that 70 percent of victim organizations had a hotline. The ACFE goes on to report that fraud losses were twice as high at organizations without hotlines. Hotlines also cut detection time by six months – from 18 months without a hotline down to 12 months with one. Tips are the best

---

9 Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*. Association of Certified Fraud Examiners, p. 22, Fig. 11.

10 Association of Certified Fraud Examiners, *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*. Association of Certified Fraud Examiners, p. 17.

11 Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*. Association of Certified Fraud Examiners, p. 27.

12 Ibid. p. 82, Fig. 85.

13 Association of Certified Fraud Examiners, *Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse*. Association of Certified Fraud Examiners, p. 19.

14 Ibid. p. 21.

indicator that something may be wrong. Organizations with a hotline received tips in 47 percent of cases against 31 percent when there was no hotline.[15]

Meanwhile, for historical purposes, the 2016 report stated that the impact of a hotline is clearly discernable when comparing detection methods with organizations with hotlines to those without hotlines.

Table 4
Impact of Hotlines[16]

Detection Method	With Hotline	Without Hotline
Tip	47.3%	28.2%
Internal Audit	18.4%	13.4%
Management Review	12.1%	15.4%
Account Reconciliation	3.9%	8.1%
By Accident	3.9%	7.8%
Surveillance/Monitoring	2.0%	1.8%
Document Examination	2.7%	5.3%
External Audit	1.8%	6.1%
Notified by Law Enforcement	1.8%	2.6%
IT Controls	2.0%	0.5%
Confession	0.9%	1.8%
Other	3.1%	9.1%

This shows us that tips from any source take the pressure off all the other detection methods. A caveat here, however, is advised. The 2016 report indicated that tips generally advise of a fraud scheme when the fraud is underway for a median time of 18 months (recall this is 14 months in the 2020 report and 16 months in the 2018 report) and there is a median loss of $150,000 (and this is $125,000 in the 2020 report and $130,000 in the 2018 report). The most effective method to stop fraud faster and cheaper is surveillance and monitoring: seven months and $44,000.[17]

Let us also consider the motivation behind the tip, whether the tip is directly through a hotline or to someone in the organization, such as an ethics officer. Frequently the tip comes from someone who learns of the fraud and is not so outraged over the scheme. They are outraged that someone is doing better than they are! For instance, an employee is padding the wallet with bogus overtime on their timesheet. Another employee learns about it. This informant calls the tip line because the perpetrating employee is buying nicer clothes, has a nicer car, and so on. I suppose for us trying to stop fraud, any reason to learn about a scheme is good. However, one wonders if the informant employee may try their own scam, figuring that the perpetrator would not have been caught otherwise. “It’s time to fill my wallet!” they might think.

Does your organization have a tip line? If so, do you believe would-be tipsters feel confident in calling the hotline? Does your organization have a policy against retaliation? What steps could the organization take to increase the comfort level of those who would call the hotline? If your organization does not have a hotline, do you believe your organization would benefit from one? How would you present it to your co-workers and assure them of confidentiality?

---

15 Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*. Association of Certified Fraud Examiners, p. 24.

16 Association of Certified Fraud Examiners, *2016 Report to the Nations on Occupational Fraud and Abuse.* Association of Certified Fraud Examiners, p. 27, Fig. 34.

17 Association of Certified Fraud Examiners, *Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse*. Association of Certified Fraud Examiners, p. 20, Fig. 11.

8. Management review

We need to start with a question regarding the definition of management review. What constitutes *effective* management review? In other words, it is all well and good for senior management to review programs, product lines, sales figures, etc., but do they truly understand what the data means?

Management must use some set of benchmarks and standards to assess performance. If a company of their size in a market of their size experiences 8 percent growth year over year at present, then seeing growth of 12 percent might be a red flag. If companies in their industry experience 18 percent turnover but their company has a turnover rate of 25 percent, then management needs to ask some tough, probing questions of folks, including looking in the mirror to assess why people are leaving. It could be indicative of a poor internal environment.

As mentioned earlier in the discussion of management certifying the financial statements, reviews may be at a very high level with not much detail. Therefore, it is far too easy to bury a fraud scheme deep within the numbers. Management reviews are but one tool in combating fraud. It should be a key control for any organization.

How does your organization conduct management reviews? Are you aware of any fraud ever being detected, even suspected, as a result of management review? How might you improve the likelihood of detecting fraud in management reviews?

9. Independent audit committee

The Sarbanes-Oxley Act emphasized the audit committee's role in establishing an internal control environment. Since passage and enactment, the performance of audit committees has been scrutinized more and more. The 2013 COSO integrated framework for internal control also has a focus on the audit committee. The key factor is that the members of the board of directors in general, and of the subcommittee known as the audit committee in particular, be independent of the organization. How do we assess that?

There is a bit of a dichotomy when it comes to independence and a paying job. Consider this: Auditor is working on the audit of Company. At some point, Company asks Auditor if the latter would consider working for Company when the audit is complete. This offer creates an issue with independence. Now, consider this: Company contacts Person to serve on Company's board of directors and quite possibly on the Audit Committee, too. If Person agrees, Person will be compensated six figures a year, plus travel, meals and incidentals, and lodging. Yet, this offer, which most likely entails much more money than the offer to Auditor, causes no apparent independence problem on the part of Person. Why is this? Person, as a board member, will have to make decisions argued for by the CEO and CFO. What if Person does not want to go along with everyone else? Sure, Person can be a dissenting vote, but how will that impact whether Person is reappointed? A dodgy company may see to it that they are not reelected.

The point is this: board members are paid well by the very organization they are supposed to be governing. I have no problem with Auditor and Company having an independence issue created by a job offer. I wonder if board members can be truly independent. And there is also this problem for the average CPA trying to reduce the risk of fraud – how does the CPA assess the independence of board members in both fact and appearance? While the external audit firm will have some access to the board, usually the manager and partner on the engagement, internal auditors may not. For instance, how does someone

assessing controls and risk at a middle level know how the most senior leadership behaves and how independent a senior board member is?

Have you ever met members of your organization's board of directors, trustees, or other governing bodies? Have board meetings ever taken place within the organization's offices so board members could assess the environment for themselves? How might you attempt to assess the board members' overall independence, especially those assigned to the audit committee?

10. Fraud training for employees

As with managers and executives above, would an increase in knowledge of fraud schemes and prevention, etc., for employees reduce the occurrence and impact of fraud? Here is something that would help managers, executives, and employees: understanding what fraud is. By that I mean this: do all personnel in the organization know that taking office supplies to use at home for personal use is a form of fraud, waste, and abuse? Do personnel realize that using the computer at work to buy presents for loved ones is a form of fraud and abuse? Now, it is possible that the company permits employees to do online shopping at holiday time or for birthday presents for immediate family? If that is the case, that is a great little perk! But still, it is an easy way fraud, waste, and abuse may occur. In essence, these seemingly minor transgressions can be the gateway to bigger schemes.

The use of cigarettes appears to be on the decline, but I can recall a time in the late 1980s and early 1990s when nonsmokers complained that smokers were getting more break time to indulge their habit. Could the extra break time smokers take today be a form of fraud, waste, and abuse if they are not working any extra time to make up for the 10-minute stretches smoking four or five cigarettes during the course of a workday? It could be anywhere from 30 to 60 minutes spent smoking in a day. It is just a thought.

What are some seemingly harmless actions (or inactions) your organization's personnel may take that upon further review are considered fraud, waste, and abuse?

How do you think co-workers would react if you were to provide training indicating that such actions can be considered fraud, waste, or abuse?

Have you ever been made aware of someone's behavior that the informant felt was fraud, waste, or abuse but you felt was harmless?

11. Fraud training for managers and executives

One may wonder whether there would be some victim organizations who would not have been victimized if their managers and executives were better trained. What might this training entail? Red flags would be one area. Typical fraud schemes that might impact their organization is another area where training would help. Perhaps the single most important training topic would be in setting the right tone at the top!

Is it not interesting that the table does not include *ethics* training? Is this to suggest that all these organizations did not have ongoing ethics training? Perhaps not. However, I would consider this an issue that my most senior people are not being refreshed in ethics. Let us face facts: the more people are exposed to bad behavior the harder it is to continue to behave properly. In essence, people who are ethical and stick to their principles early have those ethics and principles eroded over time as they are exposed to questionable behavior. "If this senior leader is padding the travel expense report and

pocketing extra cash, then why am I not taking the same advantage?" It is human nature to seek the path of least resistance. We are all susceptible. If you believe otherwise, I respectfully submit that you are fooling yourself and letting pride fool you.

Managers and executives have a pretty good handle on what the employees are paid. Managers and executives might become suspicious of someone driving an expensive car despite only earning enough to afford a basic vehicle. Caution is advised before confronting the employee or even raising a yellow flag. But training executives and managers in the warning signs of fraud as well as how executives and managers could inadvertently trigger fraud motivation is always a good thing.

Does your organization provide training to managers and executives in fraud prevention and detection? Does this training include ethics training, especially in scenarios from your organization, and/or your organization's industry? How might training in the fraud realm improve an organization's fraud defenses?

12. Anti-fraud policy

The table tells us just over one-third of United States victim organizations had an anti-fraud policy and were still victimized by fraud. It would be curious to know whether this policy was in lieu of a code of ethics and business conduct. Let us recall a very simple concept.

I was once chatting with my older son about laws. He was saying that we needed more gun control laws. I informed him, that at the time of this conversation, the United States had over 10,000 laws on the books at the federal, state, and local levels related to guns. The issue, I explained, was that criminals, by definition, do not care about the law. Therefore, passing one, a hundred, or a thousand additional gun laws would not impact *criminals*. By extension, having an anti-fraud policy will not stop the fraudster who is bound and determined to commit fraud, though it may give pause to the so-called "80 percenters" who may be tempted.

An argument can be made that getting someone to sign off on a document helps to reinforce the desired behavior. Nonetheless, a fraudster is good at lying. Therefore, signing a document affirming their reading and understanding of the document is a means to an end for them. If they were to refuse to sign it, they might lose their job, or at the very least, the direct opportunity to perpetrate the scheme. Therefore, it is logical for them to sign whatever they need to sign in order to get or maintain the position they need to be in so they can perpetrate their scheme or schemes.

Every little bit helps. Like chicken soup and oxygen for a sick person, it cannot hurt, and it might help. Does your organization have an anti-fraud policy? Is it in lieu of a code of ethics and business conduct, or is it an extension of such a code? Do you believe an anti-fraud policy would increase the likelihood of preventing fraud or of being tipped off that a scheme was underway?

13. Proactive data monitoring and analysis

There are many forms of this control, and much of it resides in the information technology realm. Perhaps one of the most telling analyses is Benford's Law of Anomalous Numbers. Physicist Frank Benford introduced this Law in 1938. He discovered that there is a distinct pattern to the digits 0 through 9 and where they appear in numbers when in the first digit position, second digit position, third digit position, etc. As a result of this law, we can analyze transactions in the accounting records and determine if there is an unusual number of instances where the number nine is in the final two places in a three-digit number to

the left of the decimal point. That is, seeing more than expected values such as 499 may indicate someone perpetrating a fraud to a level just below the $500.00 limit requiring an additional signature.[18]

Perhaps the most important word in the general control description is “proactive.” Our analysis and monitoring has to be set up to look for oddities in our expected data stream. In addition, it must be monitoring and analysis that is ongoing and persistent. In fact, it stands to reason that by analyzing smaller amounts of information every day, we may discover odd patterns faster. For example, suppose each Monday we analyze activity in a certain account for the week before. Once done, we add last week to the prior week’s data. Then we add it to the prior week’s data before that. We will soon have a month’s worth of data analyzed and may see a pattern develop as we compare each individual week’s analysis to the overall month’s amount of information. Naturally, we may catch several items in a single week where 499 appears in the account. If we take a quick look, we can assess whether this occurs because of an approval threshold.

In the digital age, we face a massive problem. As one publication states:

> In the digital world, the rules of the game have changed. Transactions happen remotely at speeds beyond human perception and on a potentially vast and automated scale. Human oversight is expensive, fallible and slow, leaving visibility on any one event or customer reduced to a degree that would have seemed incredible to businesses from the pre-internet age.[19]

Do you believe Benford analysis or other forms of monitoring and analysis would assist you in detecting fraud? Would you advocate for your organization to hire analysts whose function it was to perform such analysis?

What other forms of analysis can you suggest that would be helpful?

14. Formal fraud risk assessments

This is one control that companies may easily employ that helps reduce the risk of fraud. I would be curious to see what would happen to the U.S. and Canada victim organizations that did *not* have this anti-fraud control in place were they to ultimately initiate this control. Would they see a reduction in fraud?

It seems simple. When management makes a detailed, formal assessment of fraud risk, which is required under COSO’s 2013 internal control framework, they have a far better chance of preventing fraud. If the risk is deemed high in a certain area, they can then establish more controls. There is always the risk of evaluating the risk as low in another area where it ought to be considered high. That has always been the case. But the word formal also tends to indicate that the assessment neither takes place in a vacuum, nor is it made by one person. It leads me to believe, and perhaps you, too, that the assessment is performed by senior managers as a group. In addition, other resources may be brought to bear, including external resources such as consultants and benchmarks.

Does your organization have formal fraud risk assessments? If so, who participates in the assessments? How often do the assessments occur? If your organization does not have formal fraud risk assessments, will you advocate for them? How might you explain the benefits to their performance beyond the requirement of the 2013 COSO framework?

---

18 Huxley, S. (n.d.). *Why Benford’s Law Works and How to do Digit Analysis on Spreadsheets*. McLaren School of Business; University of San Francisco.

19 “Combating digital fraud.” (June 2014). *CIO UK*, 22. doi:December 10, 2017.

15. Dedicated fraud department, function, or team

This control also begs us to know whether companies who have such a department, function, or team are more successful in deterring fraud. The report says over one-third of U.S./Canada victim organizations in the study employed such a group. Based upon the description, it seems reasonable that these are groups of people with specialized training. They may all be certified fraud examiners (CFEs). It is also possible that this team is separate from the internal audit department, which 66 percent of United States fraud victim organizations had. The question to answer, and this would also include a cost-benefit analysis, is whether the fraud would not have been discovered without this specialized team.

The question that must also be raised is whether having a "fraud squad" sends the right message to our employees. If we establish an anti-fraud team, are we then telling our employees that we suspect them and expect fraud to occur, encouraging the behavior we seek to discourage? Would a fraudster fold up a scheme upon hearing of this fraud team? Let us also take the team members' perspective. How do they approach their job every day? Are they the internal auditors who were mandated to find fault in order to justify their existence? Might the team falsely accuse someone of fraud, waste, and abuse when, in fact, all they did was commit a simple error?

Would you consider a dedicated team such as this for your organization? How would you respond to concerns raised that you are, in essence, suspecting everyone?

We walk a very thin line between knowing that virtually everyone in the organization could be tempted to cross the line and not wanting to really reinforce that perception. If we proceed from the assumption that folks are basically dishonest, that is what the employees will be. They will live down to that opinion. Is there a way that you could introduce folks in your organization whose focus was on fraud without calling them the fraud department?

16. Surprise audits

This is one control that really seems to work. Surprisingly, only 35 percent of victim organizations in the U.S. utilized this control, and it seems that this control, like surveillance and monitoring mentioned above, can really put a crimp on fraud. Consider that anyone contemplating a fraud will have to think twice, even three times, before initiating their scheme. They would have to be meticulous in all the details to make the scheme appear honest. Those who steal rather than work for their benefits possess a lazy attitude. In essence, they are stating that it is better for them to steal five percent of their weekly salary every single week rather than perform admirably and earn a five percent raise. (Sure, not paying taxes on their ill-gotten gains factors into the equation, but it is revealing nonetheless.)

When I was in college, I worked for a retail shoe store in a mall. Right next to my store was a sister store. We sold athletic shoes, and they sold men's and women's dress and casual shoes. Both stores were owned by the same company that had several brands. We had heard that the manager of our neighbor store might be messing with the inventory. The company had an internal audit department. Each year, every store was subject to a scheduled audit and an unscheduled audit (surprise). In fact, in speaking with "Mr. Burns," the auditor assigned to our area, about what he did and how he did it, I became interested in auditing. He was a very nice man, very thorough, and tough when he had to be. Folks seemed intimidated by him, but he was a nice, smart man who seemed to perform fairly and honestly.

One day, we saw "Mr. Burns" arrive at the store next to us when the manager was not scheduled to be in. By company policy, the manager was contacted and told to come in. I will never forget the look on the manager's face around midmorning when I peeked in. "Mr. Burns" was in the back office performing his

procedures. The ashen face of the manager told me everything I needed to know. By the end of the day, the manager was terminated for cause. A locksmith arrived to change the locks. The assistant manager was told that she would be meeting a new manager the next day.

I have often felt as my career progressed that someone had called the hotline on the manager. Even surprise audits have their limitations. “Mr. Burns” did not know to look at certain transactions or inventory figures in a vacuum. He had some guidance, and with a tip the surprise audit yielded quick results.

I have employed surprise inspections in another area – labor charging on U.S. government contracts. I select a group of people to check and surprise them at their workstation. I ask a series of questions regarding their labor charging practices, assessing if they are following company and government requirements. I do it because government auditors will do it. Therefore, I was preparing my colleagues. I was always honest in my assessment of their performance and had to report to senior management on the results.

Does your organization have surprise audits? Could you start such a program? Might you hear pushback as employees may feel more like suspects?

17. Job rotation and mandatory vacation

There are two great benefits to these two policies. One is improved morale as people get to learn different aspects of the business and can fill in in case of illnesses or injuries. The other is that employees know they will use some of their accrued vacation time.

We also know from our example of Rita Crundwell in Dixon, Illinois, that oddities can appear when the person in charge of the system is away.

Does your organization encourage job rotation and insist upon employees taking vacation? If not, do you believe you could encourage your organization to adopt the programs? What other benefits might be gained by such programs?

18. Rewards for whistleblowers

Dead last on the list, in place with just 14 percent of U.S. victim organizations (though it is up two percentage points from 2020), this is probably one of the more controversial controls. To blow the whistle, tipsters have to feel their job is secure. Offering a reward for information is a long-standing favorite for law enforcement. However, it is rare that these tipsters are ever identified in public. If an employee receives a bonus for a fraud tip that leads to the detection of a fraud scheme, someone in the payroll department knows about the reward. If the employee who is caught was considered popular in the office, and fraudsters do have a way with people, the payroll employee may leak the apparent reason one employee is now gone along with who was most likely responsible for it. Before you say that would not happen, I know from experience that certain information does get passed around by many staff members that really should not be passed around.

Do you believe that rewards for whistleblowers would work in your organization if such a program does not already exist? If your organization does have this program, do you believe it to be successful, and how do you measure success? What pitfalls can you think of that would prevent this control from impacting the organization in a positive manner?

C. E-commerce fraud prevention[20]

In the digital age, added layers of controls are needed to avoid being victimized by fraudsters operating in the anonymity of the internet. Not only do we as individuals need to guard against our information being stolen, but businesses must add layers of protection for themselves. For example, a person I know noticed four charges of several hundred dollars each on her credit card to the same major technology company. She contacted that company immediately to inquire. Fortunately for her, she was not responsible for paying anything. It was unfortunate for the company, however, as they had already shipped one product. Three other transactions were halted. What additional steps can a business take to protect both their customer and the business?

1. Payment Card Industry Data Security Standards (PCI DSS)

When I first started leading courses on internal controls relative to the Sarbanes-Oxley Act of 2002, I implored those taking the class to be certain to engage their information technology personnel early and often in establishing controls. PCI DSS increases the trust customers will have in your systems. If your business has not already investigated certifying your company, then it is something to investigate. It does mean work. Retailers, merchants, or any other organization that uses electronic payments must use advanced fraud and risk management technology. There are also very strict security controls required. The payoff, like the overall cost of fraud itself, cannot be easily estimated, but not locking as many doors as possible can lead to devastating consequences.

2. Address verification system (AVS)

This is a great control because AVS is automated! It is used for transactions occurring online or on the telephone when the buyer does not physically present the card. For this to work, be sure to require the billing and shipping addresses.

3. Geolocation by IP address

Speaking of getting addresses, this one scares consumers as the merchant is getting an exact location for the buyer. However, this authentication, when combined with AVS above, adds a layer of precision. If the buyer gives an address in a state different from what the IP address is – or the address from a prior transaction does not match the current transaction in progress – the merchant can request additional information. Both this and item two above may make some consumers queasy, even to the point of breaking off the purchase. You will have to decide how best to balance fraud prevention and consumer confidence in your system.

4. Compare IP address country with billing address country

This is where “additional information” comes into play. The expectation is the IP address and delivery address are going to be in the same country as the billing address. Consumers ought to alert their bank and credit card companies when they plan to travel – especially outside their residential area or overseas. For example, I alerted my bank and credit card companies when I traveled outside the continental United States so they would know to expect transactions from Europe and when those transactions would occur. Any transaction received after the last day of my trip would be flagged. It is possible that someone may use a computer or their phone while traveling to make a purchase to have shipped to their home address or to other family members. This is where the next tile in the control mosaic comes in handy.

---

[20] “Trends in e-commerce & digital fraud: Mitigating the risks,” EKN and Radial Research Partner.

Since fraudsters are tech savvy too, they may use anonymous proxy servers to mask their actual location. This also has the advantage of making them hard to track and detect as they might appear for only a few hours in order to place as many phony transactions as possible. A fraudster in Germany may use an anonymous proxy server to appear that they are in England. While difficult to detect, we can attempt to reduce risk.

This is done in a layered approach. We take the domain, proxy, ISP, and host data center data to see if the connection is suspicious. There are various IP intelligence providers with a range of options. Spending extra for a high-quality system might be the best approach if you wish to employ this system. Choosing a weak or outdated system might be the same as spending a great deal of time cleaning your floor only to place a dirty welcome mat at your front door.

5. Card verification value (CVV)

The CVV is that three-digit number on the signature box of your credit and debit cards. (Some companies may use four digits and place the number in other places, and they may refer to it by a different acronym.) The CVV is not stored on the magnetic strip! This means that someone must have the card in their possession to read the number.

6. Security services

This is basically a type of trust mark service that scans your system each day in search of any malware or other vulnerabilities. It is an added layer of protection. The most common security services in the market now are Verisign, TRUSTe, and McAfee. The presence of such indicia on your website serves the same purpose as having an alarm company sign in front of your home and on windows and doors. It sours the target for potential thieves.

7. 3-D Secure

This focuses on the online credit and debit card use. With this, the card user is required to enter a unique password provided by the card issuer that is supposed to be known only by the card holder.

8. Enable secure login

These credentials are for your customer. They set up their account and use it with you. The merchant's advantage is being able to market to their customers directly and understand buying patterns. When a transaction breaks a pattern, then it is time to contact your customer to ensure the purchase is legitimate.

D. Digital twins[21]

The concept of a digital twin is simple. Let us say, for example, that I manufacture jet engines. Using software, I create a digital version of the engine, incorporating a virtual version of every single component necessary to allow the engine to function properly. I then program the computer to run that engine through its paces to see what will go wrong and when. Using this data, I can alert mechanics to check real engines on real jets for these problems before they exist.

Based upon this model, General Electric (GE) and Ernst and Young's (EY) Fraud Investigation and Dispute Services, known as FIDS, decided to utilize this concept on people. That is correct. EY and GE created a digital twin of GE employees to assess when the employee would become vulnerable to

---

[21] This section is based upon: Walden, V. M., CFE, CPA (Ed.). (January 2018). "'Profit & Loss-of-One': Preventing fraud, enhancing compliance using digital twins." *Fraud Magazine*, *33*(1), 58-69.

compliance issues. The genesis of the project was the observation that GE personnel took their requisite training, but the powers that be in the compliance department questioned how effective the training was. They asserted, and I concur with this assertion, that the training was, in their words, a "check the box" exercise. The employees were not retaining the information.

Let us be honest. How many times do we "attend" a course: (1) because it is required; and (2) when there, essentially ignore what is going on around us until it is time to receive the certificate? In fact, a few years ago I once led an eight-hour class on internal controls attended by four government employees who did not need to know about the Sarbanes-Oxley Act of 2002 as their organization was exempt! Why did they show up? They were already at the hotel for a conference and this course offered eight continuing education credits. All four were on their laptops while I presented the course live to folks "attending" by way of a webcast. I can only imagine what the folks online were doing.

Did anything I said that day stick with anyone? I tend to doubt it. GE's compliance team felt that compelling people to attend classes when they were not relevant to everyone attending meant that many folks were checking out mentally rather than paying attention. Later, when the subject matter really did matter to those people, the course was checked off as taken. In the example presented in the article, a fictional employee's history with GE is captured along with the person's present role and anticipated future activities. This "P&L-of-One," as it is called, maintains and updates the information with feedback from the employee. When the employee is scheduled to travel overseas for the first time in order to visit a customer, also for the first time, where the customer is 75 percent owned by the foreign government, the "P&L-of-One" sends a message to the employee in the preferred manner of the employee (text, email, or other method) to advise that the employee ought to take a course on GE's ethics policies relative to foreign travel and bribes masquerading as normal business practices in a foreign country.

This "just-in-time training" approach is only the first layer in overall compliance and instilling GE's overall desire for ethical behavior. The system also tracks employees' response to the messages. If an employee ignores "suggested" training, the messages may become more directive to require training. The article provides this insight to the future:

> The P&L-of-One pilot could be a significant step in demonstrating how a company's digital transformation initiative can benefit the compliance function. … For example, next to just-in-time training and communication, real-time data and behavioral analytics can be powerful tools in other risk control areas such as anti-fraud and anti-corruption.[22]

The article does not address how GE employees took the news that data was collected for this purpose. In the digital age, reducing one's digital dust becomes more complicated as more and more repositories of data are created. This is another potential gold mine for hackers. Such is the world in which we live.

---

[22] Ibid. p. 69.

Fraud's New Frontier

Fraud's New Frontier

Learning objectives

Upon reviewing this chapter, the reader will be able to:

- Understand the growing emphasis on entities' environment, social, and governance reports;
- Understand that publicly traded companies are not the only organizations that may be required to issue these reports; and
- Realize that if the reports are added to financial statements, as auditors we may not be "competent" to opine on these reports.

I. Introduction

In early 2022, the Harvard Law School Forum on Corporate Governance posted an article titled, "Best Practices for Establishing [Environmental, Social and Governance] ESG Disclosure Controls and Oversight." The authors state at the top, "the demand for information regarding companies [ESG] activities, risks and opportunities has risen sharply."[1] You may already be aware that the United States House of Representatives passed a bill in 2021 that would require companies registered with the Securities and Exchange Commission (SEC) to include such reports in their filings. However, as the article referenced above states on page 3, "some institutional investors have begun discussing the potential desirability of third-party assurance of some ESG data."[2] You may wish to take a deep breath.

On March 21, 2022, the SEC released a 510-page document with proposed rules regarding how public companies will have to report on climate change risks posed by their company. The disclosures were to be part of the audited financial statements! Commission Chair Gary Gensler posted a statement on the SEC website. In it he stated, "I am pleased to support today's proposal because, if adopted, it would provide investors with consistent, comparable, and decision-useful information for making their investment decisions and would provide consistent and clear reporting obligations for issuers."[3] Mr. Gensler goes on to cite studies and surveys about investor demand for such information. He then stated, "I am guided by the concept of materiality. As the Supreme Court has explained, information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment or voting decision, or if it would have 'significantly altered the total mix of information made available.'" (See *Basic Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988).) We will look at materiality below in Section III.

Immediately after the comments quoted above, Mr. Gensler states clearly:

> The proposed rules would require disclosures on Form 10-K about a company's governance, risk management, and strategy with respect to climate-related risks. Moreover, the proposal would require disclosure of any targets or commitments made by the company, as well as its plan to achieve those targets and its transition plan, if it has them.[4]

---

1 Bell, D. A., & Llewellyn, R. C. (February 3, 2022). "Best Practices for Establishing ESG Disclosure Controls and Oversight." Harvard Law School Forum. Retrieved March 7, 2022, from www.corpgov.law.harvard.edu/2022/02/03/best-practices-for-establishing-esg-disclosure-controls-and-oversight.

2 Ibid.

3 Gensler, Gary (March 21, 2022). "Statement on Proposed Mandatory Climate Risk Disclosures." Retrieved March 24, 2022, from www.sec.gov/news/statement/gensler-climate-disclosure-20220321.

4 Ibid.

Forbes posted an article two days later asking, "Will the new SEC climate disclosure rules matter?"[5] The contributing author believes this to be "a really big deal." Moreover, she writes that "[i]nvestors have been clamoring for this information for years, especially those who prioritize companies that are disclosing their risks to climate change…"[6] Simply stated, four things would be reported:

1. What the risks are to their business from climate change. This would include risks to operations, strategy, and future.
2. What the company is doing to mitigate those risks. The *Forbes* article author suggests things such as relocating plants (out of "Tornado Alley," for example) or shoring up plants to mitigate damage (for instance, if the plant is in the southeastern United States and is therefore susceptible to hurricanes and tropical storms). Perhaps they want to alter strategies and decide what strategies are employed to determine mitigation of risks.
3. What the company's greenhouse gas (GHG) emissions are presently and anticipated to be in the future.
4. If the company has stated goals publicly (for example, they have declared they want to be net zero by 2030 or 2050), the company will have to report its transition plan in the financial statements with the impact to the business during the transition period.[7]

The SEC had previously provided a sample that would be sent by the Division of Corporate Finance. This sample letter spawned from guidance issued some twelve years ago. It is based on "Disclosure matters discussed in the 2010 Climate Change Guidance… ." There are three points:

- The impact of pending or existing climate change-related legislation, regulations, and international accords;
- The indirect consequences of regulation or business trends; and
- The physical impacts of climate change.[8] [*sic*]

While the SEC proposed rules are new, this type of reporting is not. In fact, one can find corporate social responsibility (CSR) reports going back more than a decade. Harvard Business School Online blog author Catherine Cote defines them as, "…an internal- and external-facing document companies use to communicate CSR efforts and their impact on the environment and community."[9] Within this article, the author provides five links to CSRs (though when your author attempted to connect to the fifth, Warby Parker's 2018 impact report, there was an error). These reports were highly produced – full color photos, charts, and graphs throughout the document. And these reports were long! The General Motors 2019 report was 179 pages! One can imagine an auto manufacturer would have a lot to discuss relative to climate and sustainability. IBM's report weighed in at 70 pages, while Cisco was close behind at 68 pages. Walt Disney was the briefest of the bunch at 42 pages. However, adding bright color and open page space may add to the length, but readers will be more impressed with the text.

---

5 Michaelson, Joan (March 23, 2022). "Will The New SEC Climate Disclosure Rules Matter?" *Forbes*. Retrieved March 24, 2022, from www.forbes.com/sites/joanmichaelson2/2022/03/23/will-the-new-sec-cliamte-disclosure-rules-matter.html. NB: "The statements in this guidance represent the views of the staff of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the [SEC]."

6 Ibid.

7 Ibid.

8 SEC (September 22, 2021). "Sample Letter to Companies Regarding Climate Change Disclosures." Retrieved March 24, 2022, from www.sec.gov/corpfin/sample-letter-climate-change-disclosures.html.

9 Cote, Catherine (April 20, 2021). "What is a CSR Report & Why is it Important?" Harvard Business School Online. Retrieved March 24, 2022, from www.online.hbs.edu/blog/post/what-is-a-csr-report.html.

The author provides some advice for improving efforts in CSR reporting. Cote writes:

> Harvard Business School Professor Rebecca Henderson implores professionals to start with a purpose and build the business case from there. What's an issue that impacts your business, customers, or community? Start by identifying a cause that's important to members of your organization, and then brainstorm a quantifiable goal you can set that would help that cause.
>
> To make the business case to skeptical members of your team, consider the publicity value, customer and employee loyalty, and return on investment of committing to a sustainable or socially impactful cause.[10] [Hyperlinks within omitted]

Question to ponder:

Does this suggestion from Harvard Business School sound more like *marketing strategy* than *financial reporting* requirements? If you believe it to be the former, how often are CPAs engaged to test marketing strategies – not the costs – in financial statement audits? If you answer, "Rarely, if ever," you may well be correct. If you believe the latter, because such reports would become part of the financial statement audit, when SEC rules go into effect, how might the "publicity value, customer and employee loyalty, and [especially] return on investment" be quantified? (Materiality will be discussed below in section III.)

Here is some further background information. In 2018, Cidel Asset Management wrote what amounts to a white paper titled, "The Rise of ESG Disclosure and What It Means for You & Corporate Governance Explored." The report states, for instance, "As of 2017, 75 percent of major companies around the world produced some form of CSR report, up from 19 percent in 2002."[11] [*sic*] Cidel goes on to suggest that these reports may assist management in seeing that excessive pollution discharges into the environment may be due to inefficiencies that might harm the profit margin.[12] That is a topic for management, and Cidel believed that such reporting is of interest to investors. If we CPAs are to opine on the ESG/CSR, however…

As astronaut Jim Lovell famously said in the cool, collected manner one might expect from a seasoned Navy pilot, "Houston, we have a problem." If the cost of audits jumping with the enactment of the Sarbanes-Oxley Act of 2004 shocked auditees, imagine the potential for cost increases adding ESG/CSR to financial statement audits! What is the problem? Let us look.

II. Competence

Your humble author has stated to several colleagues that one cannot audit what one does not understand. The first time doing so was to two U.S. government auditors who were both CPAs. They asked one of the most astounding questions: "Why are there positive and negative amounts in the general ledger accounts?" You laugh. But they were *serious*! The reply was measured, as your author suppressed the extreme desire to laugh. "In a computer-based accounting software debits are positive numbers and credits are negative numbers, which is why the trial balance nets to zero." All hope that they were merely trying to assess *my* abilities, seeing if the answer given was "Gee, I don't know" was quickly erased. "Oh, we never realized that." That was the first time your author said, "you can't audit what you don't understand."

---

10 Ibid.

11 Cidel Asset Management (December 2018). "The Rise of ESG Disclosure and What It Means for You." Retrieved March 21, 2022, from www.cidelinstitutional.com.

12 Ibid.

A. History teaches us

Perhaps the most infamous case of CSR/ESG fraud is that of car maker Volkswagen. The story started in 2008 when Volkswagen announced they were introducing “clean diesel” cars. Outside of a select few within the company, no one knew that the vehicles had a secret. The cars, initially sold in the United Kingdom, had a special software built in to fool emissions testing devices. Sales of diesel cars had been on the wane, and a select few within Volkswagen, desperate to produce a rebound in sales, hatched a plan to boost sales. The following year, the vehicles hit the U.S. market. It seems Volkswagen had turned their sales around.[13,14] The plan began to unravel as environmental groups grew frustrated at the disconnect between testing data and real-life data. In 2014, the International Council on Clean Transportation commissioned a study that found there was a discrepancy between what the company claimed and the actual performance in road tests. It took a year-long investigation to uncover a segment of computer code quaintly labelled "acoustic condition” as the defeat device.[15]

Careers were ruined. Money was lost. Reputations were severely damaged. Volkswagen’s auditors never uncovered what could have been described then as “revenue fraud.” Even if they looked at the test data, could a certified public accountant truly understand it?

B. ESG and the CPA

Let us begin by stipulating that few, if any, CPAs would be able to effectively test a car’s engine to have reasonable assurance that the claims made by the car manufacturer are true. A CPA may audit a car manufacturer. The auditor can understand the business cycle – parts in inventory, work in process, finished vehicles ready to ship, in-transit, arriving at the dealership, interest receivable and received, and liabilities for dealership rewards for selling units. How can that auditor truly assess statements made by the manufacturer about the environmental friendliness of the engines?

But that is not all. There are two other facets to ESG – the S and the G. The latter, governance, we ought to be assessing as part of the audit now. We will not spend more time on that one. We do have to assess *social* somehow. Social includes diversity, equity, and inclusion (DEI). It will also include other elements of “social,” such as charitable giving, community outreach, and supporting employees’ charitable opportunities. More is presented below in Section IV.

There are too many other factors to address. Fortunately, we have an overseer to assist us and our clients.

C. The Sustainability Accounting Standards Board (SASB)

Yes, this board is real. Following is the description from the SASB website:

> SASB Standards identify the subset of environmental, social, and governance issues most relevant to financial performance in each of 77 industries. They are designed to help companies disclose financially-material sustainability information to investors.

---

13 UK Volkswagen Group (August 1, 2008). “The Passat.” Retrieved March 7, 2022, from www.volkswagen.co.uk/assets/commpon/pdf/brochures/old-brochure/Passat-Saloon/Passat-Saloon-August-2008.pdf.

14 UK: Volkswagen Group (July 1, 2009). “The Passat Estate.” Retrieved March 7, 2022, from www.volkswagen.co.uk/assets/commpon/pdf/brochures/old-brochure/Passat-Estate/Passat-Estate-July-2009.pdf.

15 Phys.org (May 22, 2017). “Researchers find computer code that Volkswagen used to cheat emissions tests.” Retrieved from www.phys.org/news/2017-05-code-volkswagen-emissions.html.

> SASB's rigorous and transparent standard-setting process includes evidence-based research, broad and balanced participation from companies, investors, and subject matter experts, and oversight and approval from an independent Standards Board. Supporting materials related to the development of the standards are available in the Standard-Setting Archive.[16]

It is worthwhile to check out the site and search for additional information and resources. The key takeaway in this section is that ESG reports will not be just for large, publicly traded companies. A driving force will be banks and other lending institutions. ESG reporting will be part of loan covenants – you may have come across this already! Review the standards referred to above and begin to consider how your clients, or your business if you are in the private sector, may come under ESG reporting requirements.

Questions to ponder:

Are you aware of any experts your practice or organization can access to assess ESG elements? What specific areas will challenge you the most in terms of gathering information for the ESG report and supporting the assertions made within it? Are there any other experts you can think of that could help your organization?

III. ESG examples

A. Overview

For this section we will review a couple examples of ESG report elements using information from the Environmental, Health, and Safety (EHS) Management blog. The blog is operated by a company called Perillon. According to their website, "Perillon is a simple, affordable EHS management software that centralizes all your regulatory compliance, enterprise risk, and sustainability data and activities. So you can save time, reduce risk, and prevent unwanted events."[17] [*sic*] Perillon used examples from several of their clients in a blog post titled, "4 ESG Report Examples to Get You Started With Your Own." That is, writing your own ESG reports.

Let us look at the first example Perillon presents from their customer National Grid. As Perillon states in the blog post, "The content of this 67-page report is extremely detailed."[18] Perillon also points out that National Grid has been producing an ESG report since 2001. Perillon provides the advice that when writing your report, consider your audience. Perillon wrote, "A report that's geared toward consumers will contain different information than one that's written for investors or shareholders."[19] National Grid's report included information on energy efficiency. Quoting from a snippet of that report included in the blog post:

> In June 2020, Niagara Mohawk Power Corporation, which owns and operates electricity distribution and transmission facilities in upstate New York, issued a green bond for $600 million. Just over 5 percent of this amount is being invested in energy efficiency programmes, including energy storage projects which are estimated to deliver annual savings of 36 MWh.[20]

What are "green bonds"? Like any other bond that is issued, they are fixed income instruments that specifically support climate-related or other environmental projects. Mostly issued by the World Bank, green bonds may come with certain tax advantages.[21] Can you see now how the hook is baited? Your

---

16 SASB website accessed March 12, 2022. https://www.sasb.org/standards/download/.
17 Perillon website accessed March 12, 2022. www.perillon.com.
18 Niemoller, Jim (September 14, 2021). "4 ESG Report Examples to Get You Started With Your Own." Perillon/EHS Management Blog. Retrieved March 7, 2022, from www.perillon.com/blog/esg-report-examples.html.
19 Ibid.
20 Ibid.
21 Segal, T., Scott, G. and Munichiello, K., 2022. "What Is a Green Bond?" *Investopedia*. Retrieved March 17, 2022, from https://www.investopedia.com/terms/g/green-bond.asp.

company or your client(s) are large enough to issue a bond, and a green bond issue is going to carry positive appeal, but somehow the actual benefits promised will have to be authenticated. What if the green bonds were issued for a phony green project?

Now, let us assess what the electricity savings, if realized, mean.

The average household in the U.S. uses 10,716 kilo-watt hours (kWh) of electricity each year. Obviously, usage can be above or below that average depending on where one lives in the country. But National Grid was talking in terms of mega-watt hours (MWh) – saving 36 MWh. Simple math converts the average U.S. usage to 10.716 MWh. This means the proposed savings is the equivalent of just over 3 $^{1}/_{3}$ U.S. households, or about 3.36 to be more precise.

One way to address the question is to assess materiality. Fortunately, Perillon includes this discussion on the blog.

> ESG materiality refers to whether or not [*sic*] a piece of information is relevant and important to a company's environmental, social, and governance reporting. If an item is material, it should be included in the company's sustainability report. If not, it should be left out.
>
> Materiality is a term that is used in many different contexts, including law, auditing, and accounting. Different contexts may apply the term in slightly different ways. For example, materiality in accounting refers to the relative size of an amount, with relatively large amounts of money being considered material and relatively small amounts immaterial. The common thread is that materiality refers to whether or not [*sic*] something is both relevant and important, or 'material,' to the issue at hand.[22]

The first question is whether the information about saving 36 MWh is important to the report's *readers*? Since it was included, we can assume that it was deemed relevant and important to National Grid's ESG report's readers. Does it change, however, whether the readers are Niagara Mohawk customers in upstate New York or if the readers are green bond holders in the UK? Suppose the readers are elsewhere in the U.S. Suppose the readers are at the Environmental Protection Agency.

Let us introduce another term that we as auditors would be expected to be looking for in a report. Perillon writes in the blog, "Investors and regulators are increasingly scrutinizing companies' ESG disclosure for signs of greenwashing, so having access to detailed sustainability data is a must." [Underscore and hyperlink not included.] Greenwashing is the same as whitewashing – trying to fool people that facts or circumstances are not as bad as they appear or that what is reported is much better than it appears. Suppose someone thought the MWh savings discussed above was interesting but irrelevant? Might that person accuse the company of "greenwashing"? How might you feel if you were the auditor?

Another example provided by Perillon focuses on Energy Recovery, Inc. In this case, Perillon provides a screenshot from Energy Recovery's ESG report whereby Energy Recovery discusses a new pressure exchanger device that will "contribute to reducing water scarcity and promote more affordable access to clean water."[23] This is another example of a claim made that may indeed have experiments to support the claim, but is a CPA capable of repeating the tests and experiments to validate the claim? Is it enough to

---

22 Niemoller, Jim (June 29, 2021). "What is ESG Materiality." Perillon/EHS Management Blog. Retrieved March 12, 2022. www.perillon.com/blog/what-is-esg-materiality.html.

23 Niemoller, Jim (September 14, 2021). "4 ESG Report Examples to Get You Started With Your Own." Perillon/EHS Management Blog. Retrieved March 7, 2022, from www.perillon.com/blog/esg-report-examples.html.

observe a re-test? We CPAs do make observations as part of our audits. We observe an accountant retrieve reports from the accounting system. We observe someone in accounts receivable try to access the cash receipts module in the software. We never question the keystrokes. We trust the report produced is exactly what it ought to be. We trust there is no "bug" in a system that allows a false screen to pop up and indicate the AR clerk cannot access the cash receipts when, in fact, they can. Should a CPA engaged to opine on a company's ESG expect to watch water run with and without that new pressure exchanger?

This comes down to the AICPA *Code of Professional Conduct* 1.300.001.01 a., which states, "Professional Competence. Undertake only those professional services that the member or the member's firm can reasonably expect to be completed with professional competence."

B. Example

Now let us take a practical approach. For this example, suppose you have a client that provides residential housecleaning services. The client has cars that are painted and decaled with business information. The client has a line of credit with a local bank that wants ESG/CSR/DEI. You now must audit the books, but you will also need to assess the ESG/CSR/DEI report. Your client has included a statement that the company will transition to an all-electric vehicle fleet over the next two years. The first step you may want to take is to compare the traditional gas-powered car to the all-electric car.
Early in the 21st century, the Environmental Protection Agency (EPA) needed a way to assess an electric vehicle compared to a gas-powered vehicle. The EPA determined that 33.7 kWh was the same amount of energy content as one gallon of gasoline. This means that an electric vehicle that uses 33.7 kWh to go 100 miles rates as "100 miles per gallon equivalent", or 100 MPGe.[24] There is something else one needs to know about the difference between electric and gasoline vehicles – fuel efficiency is reversed. This means that the typical gasoline-powered engine is more fuel-efficient during highway driving and less so city driving. Electric vehicles are more efficient for city driving than for driving at higher speeds. How does one compare apples to oranges? The answer is by adjusting one to the other. That is what you would do to analyze your client's idea of flipping the fleet of cars.

First, we must gather certain information. For simplicity's sake, we will stipulate that the vehicles your client wants to acquire use 33.7 kWh to go 100 miles. The cars being replaced average 33.7 MPG and have a fuel tank capacity of 15 gallons of gasoline. Let us look at some quick math: [25]

Electric Vehicle	Gasoline Vehicle
33.7 kWh	15-gallon tank
Range = 100 miles	Range 505.5 Miles (33.7 x 15 gal)
2.97 miles per kWh (100 / 33.7)	33.7 MPG
Cost to Recharge $0.55/kWh (15 minutes)	$3.95/gallon (~10 minutes)
Total cost per refill $18.54 (33.7 kWh x $0.55/kWh)	$59.25 (15 gal x $3.95/gal)
Cost to Match Gasoline Range: 33.7 x 5 Recharges = 168.5 kWh plus 2 kWh to approximately equal 505.5 miles; 170.5 kWh x $0.55/kWh = $93.78	In order for an electric vehicle to travel about the same distance, it will cost about $34.53 *more* than the gasoline engine.

[24] Ganz, Andrew (September 8, 2021). "What is MPGe? Everything You Need to Know." Kelly Blue Book. Retrieved April 7, 2022, from www.kbb.com/car-advice/what-is-mpge.

[25] Vincent, John M. (August 27, 2021). "How Much Does it Cost to Charge an Electric Car?" Retrieved April 7, 2022, from U.S. News/Cars www.cars.usnews.com/cars-trucks/electric-car-charging-costs.html.

Another factor to consider is the price of EVs. The 2023 Chevrolet Bolt EV has a sticker price of $26,500. One can prepare for an EV to cost 33 percent more than an equivalent non-electric vehicle. The average price in the U.S. is around $70,000.[26]

Before we dismiss all-electric vehicles entirely, EVs are well-suited for short trips in cities and urban areas. Commercial charging stations in these areas can recharge much faster than the charger one may have installed at home. Consider that the installation for a home charger will cost $1,200 or more, and recharging is not as fast as commercial direct current chargers. You can learn more about this by reading the U.S. News article referenced. By the way, if you are wondering, the cost of a gallon of gas that would break even with the EV is $6.246295 per gallon. At that price point, it would cost $93.69 to either charge the EV or fill a gas tank with 15 gallons of gasoline.

IV. Social

We mentioned this aspect above in Section II. B., but let us look a little deeper into what may be the hardest aspect of ESG/DEI. Social reporting covers two areas: the company's relationships with its employees and the societies in which it operates. Within both areas is the impact of the political environments where the company operates.[27] S&P Global's article also highlights two other areas. The first area refers to the social factors that may impact both short-term and long-term goals. The second area refers to the various social factors influencing investors and the public, including "a company's strengths and weaknesses in dealing with social trends, labor, and politics."[28]

The economy and conflicts outside the United States may influence societal risks for the company's ESG report. S&P's article summarized these factors:

- How can a company's workforce requirements and composition present problems for the organization in the future? Labor strikes or consumer protests can directly affect a company's profitability by creating a scarcity of skilled employees or controversy that is damaging to a corporation's reputation.
- What risks come with the safety implications of a product or the politics of a company's supply chain? Corporations that ensure their products and services do not pose safety risks, and/or minimize the exposure to geopolitical conflicts in their supply chains tend to face less volatility in their businesses.
- What future demographic or consumer changes could shrink the market for a company's products or services? Complex social dynamics, from surges in online public opinion to physical strikes and company boycotts by different groups, affect long-term shifts in consumer preferences. Decision-makers can consider these as important indicators of the company's potential.[29]

One could not summarize the factors any better. However, one issue must be added since this article appeared less than a month before the sudden acute respiratory syndrome coronavirus 2 (SARS-CoV-2), also known as the coronavirus identified in 2019 (COVID-19) global lockdowns. There are now workers who want to work from home as they did during the lockdowns. The movement has been nicknamed the Five-O. This means no more five days in the office (Five-O now means "five over"). (See also the Surgent

---

26 "Electric Car Prices: The Average Electric Car Cost in 2023." Retrieved February 6, 2023, from www.findmyelectric.com/blog/electric-car-prices.

27 S&P Global (February 24, 2020). "What is the "S" in ESG?" Retrieved March 21, 2022, from www.spglobal.com/en/research-insights/articles/what-is-the-s-in-esg.

28 Ibid.

29 Ibid.

course ICC4, a four-hour CPE course titled “Internal Controls, COSO, and COVID-19,” which discusses, among other things, work-from-home arrangements.) Your organization may already be dealing with this issue. There is an upside to working from home – no commute. Using gasoline harms the environment. Taking cars off the road permits cars on the road to be more efficient with reduced traffic. Even better, the reduced number of cars permits trucks to keep moving at a more fuel-efficient pace. It is, in some sense, a win-win scenario.

Diversity, inclusion, and equity are quite natural. One need only look out a window and see diversity in nature. There are millions of different species of birds, mammals, reptiles, amphibians, insects, and other animals of vastly different sizes just as there are plants ranging from small flowering weeds to beautiful roses, shrubs, and trees of all kinds. The ability to see such diversity in nature depends on where one lives. What inhibits “diversity”? One could decide to kill all the grass and other vegetation on one’s land, leaving only dirt and rocks. That alone would discourage small animals from inhabiting the area. Raptors would not sail overhead. Some insects, though, may find it habitable. This may attract certain types of birds or other insects. What about in our workplace? Often, it comes down to having blinders on, just like those worn by racehorses to keep them focused on what is ahead rather than what is beside them. It limits our vision.

Real-world example:

Your author is not only a CPA, but an actor as well. I have performed in several plays, was nominated for a best actor award, and appeared in two films and a streaming series. Not long ago, I had the chance to be a stage manager for an outdoor theater production. Having never stage managed before, it was a new challenge and a remarkable experience. When the chance to pitch to direct a show came up, I jumped on it. I got the directing gig. Now, I had to cast the show. Step one was to hold open auditions. I had about 28 people audition for a total of four roles – two male and two female, all four appearing to be late-twenties to mid-thirties. My job as director was clear: find the best four actors to fill the roles. After open auditions, I called back five men and three women. After the callbacks, and they had all left, I felt like the loneliest *person* in the world. They were all so *good*! Consulting with the producers, I chose my cast. (The cast were phenomenal!) Focused on finding the best actors, here is the cast I selected: a 20-year-old single, straight Latino man, a 34-year-old gay married man with spina bifida, a 30-year-old single, straight woman of Anglo-Saxon descent, and a 33-year-old woman, who is married to a transgender woman, and she, too is Latina.

Your author never knew any of the “identity” details (and never cared) when they auditioned. The show evolved into a smash hit! When one seeks talent and ability, one finds diversity. It is natural.

If you are in the situation of making hiring decisions, whether for employees or subcontractors, or anything else, look for the best and assess whether you may have a bias, even a subtle bias, before beginning the process. But when you are auditing a client, can you determine whether your client is open to anyone and everyone who is qualified to work for them? How can you determine if your clients’ ESG report, which may have a subsection dedicated to DEI, is being honest? Organizations will say what must be said. Consider the discussion above citing S&P Global’s article. No person or company *wants* to be “canceled.”

We do have audit steps in place to assess if there are any liabilities that may have to be booked, such as a pending lawsuit. Such a suit may be over hiring practices. If your client will not talk about it even in broad terms, there may be another, bigger problem. Would this not have to be disclosed in both the Notes to the Financial Statements and the ESG/DEI?

V. Conclusion

There is clearly a move towards more disclosures related to an organization's climate impact. Investors have high interest in these disclosures, not just from public companies. Consider bank's or other lending institution's own disclosures in the loans written to climate-friendly companies. If you audit banks or credit unions, will you have to take additional steps to gain comfort with their procedures? How will you assess their decisions to make or deny loans based on climate impact or lack of DEI? Have calls been made or emails sent to the client's fraud hotline or ethics hotline? Consider planning early for both your clients and your business.

Summary

We have covered quite a lot in our discussion of fraud. The approach from the outset was not to discuss specific fraud schemes, though some were mentioned. We did not want to focus exclusively on internal controls, though we did review controls that were supposedly in place at victim organizations. Rather, we wanted to get to the root causes of fraud. While it's true that nearly everyone may be capable of perpetrating some fraud, even something that is wasteful, abusive, and petty compared to the major fraud schemes we mentioned, we must not send the signal that we may suspect everyone too strongly, lest we encourage the very behavior we wish to prevent.

We also touched on other factors that might push someone toward committing fraud. The economy and pressures created by the organization itself could inadvertently trigger bad behavior. We took the discussion further to include so-called deviant behavior in the workplace as an indicator that someone *may* be committing fraud. They may be very adept at hiding the fraud, but their deviant behavior is so deeply ingrained that they cannot hide it.

We considered anti-fraud controls, which, ironically, were in place and presumably designed and operating effectively within fraud victim organizations. What this tells us is that even with strong internal controls we are probably being victimized right now by our employees. That is why inadvertently giving the impression that we suspect everyone is so difficult to avoid.

No single set of controls will work for every organization. Size may preclude strong segregation of duties or an internal audit department. Even so, there can be other controls put in place, such as management review, that can mitigate the risk of fraud. Such review ought to include review of bank statements and credit card statements.

And just when we thought we might have a handle on it all, we added a new facet to organizational reporting and audits – ESG/CSR/DEI reports.

Ultimately, we must accept the fact that there is at least one fraud scheme underway in all organizations right now. It may involve payroll, billing, expense reimbursement, or other schemes, but at least one is underway today! Being proactive in our fraud prevention program is critical. We cannot sit back and hope we catch a fraud. We must be willing to provide an easy means of reporting fraud, such as a tip line or a hotline, and use analysis to assess whether the numbers add up. The proactive analysis may include detailed analysis using Benford's Law or other forms of data review. Our benchmarks and standards ought to be selected wisely to make our analysis more robust. Most importantly, the analysis must be persistent. We cannot take time off from it. The data we gather must build upon each layer of data. We create a mosaic that provides a clearer picture of our performance. Even an otherwise picture-perfect performance measured against the benchmarks and standards must withstand additional scrutiny.