Fraud Case Studies: Schemes and Controls

FRD4/25/V1

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.

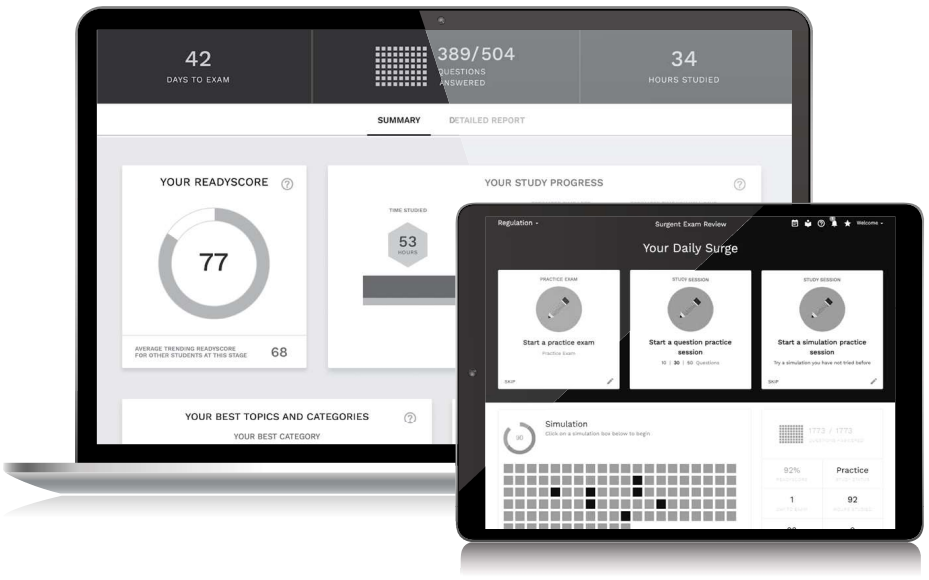
(484) 588.4197
salesinfo@surgent.com

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 April 2025

NOTES

Introduction

Introduction

Learning objectives

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

- Understand why a general understanding of internal controls is needed;
- Understand those controls may not be as solid as thought; and
- Realize that the "name" in fraud, Ponzi, may have a new method of taking money.

I. Two foundational topics

Some material, such as what we discuss in this course, requires a set of knowledge to be better understood and appreciated. Gaining that knowledge beforehand helps you with this material. You may recall from either the eight-hour course *Winning the Fraud Battle in the Digital Age: Prevention and Detection* (CFVV), or its two four-hour segments *Fraud Basics: Protecting the Company Till* (DRF4) and *Proven Controls to Steer You Clear of Fraud* (FFC4) that we discussed two general topics. First, fraud victim organizations had controls in place, and second, that there are reasons that good people go bad. That foundational understanding will be built upon in this course.

Fraud victim organizations reported fraud even though they had as many as 18 controls in place, apparently tested and deemed effective in both design and performance. Yet, those controls apparently failed to prevent and/or detect fraud. One reason we cited was that many of the controls were "soft"; meaning difficult to gain concrete evidence that they were being followed. As mentioned then, and we want to reiterate here, someone perpetrating fraud will do whatever is needed to hide their scheme. The fraudster will gladly sign a certification that he or she has read the code of conduct and ethics and understands it fully, or that the financial statements are stated fairly in all material effects. All the while, the scheme is either percolating or well underway.

Let us review the 18 controls listed below and try to assess whether the control is "soft", "evidentiary", or both. A "soft" control has little or no hard evidence. Just because the code of conduct exists, we rely on people to certify that they read, understand, and will actually adhere to it. Naturally, evidentiary controls have supporting documentation to provide some assurance that the control was performed properly and completely.

Here are the 18 controls. On the next page, we present what general type (soft or evidentiary) of control your author believes it is.

External audit of financial statements
Code of conduct (ethics)
Internal audit department
Management certification of financial statements
External audit of internal controls over financial reporting
Hotline (tipline)
Management review
Independent audit committee
Fraud training for employees
Anti-fraud policy
Fraud training for managers/executives
Employee support programs
Dedicated fraud department, function, or team
Formal fraud risk assessments
Proactive data monitoring/analysis
Surprise audits
Job rotation/mandatory vacation
Rewards for whistleblowers

Control	Soft	Evidentiary
External audit of financial statements		X
Code of conduct (ethics)	X	
Internal audit department	X	X
Management certification of financial statements	X	
External audit of internal controls over financial reporting	X	X
Hotline (tipline)	X	X
Management review	X	
Independent audit committee	X	
Fraud training for employees	X	
Anti-fraud policy	X	
Fraud training for managers/executives	X	
Employee support programs		X
Dedicated fraud department, function, or team	X	X
Formal fraud risk assessments	X	X
Proactive data monitoring/analysis		X
Surprise audits		X
Job rotation/mandatory vacation		X
Rewards for whistleblowers	X	

Notice, dear reader, that your author believes most of the controls are “soft.” A few are both. Even fewer are “evidentiary.” What “softens” an internal audit department? Consider: Are the personnel charged with internal audit *given authority to perform the audit function*? Are the internal audit engagements properly planned and supervised? Are the workpapers of high quality? You may add your own. The same is true of the external audits of financial statements and internal controls over financial reporting; as well as a dedicated fraud (prevention) department, function, or team.

How do we assess the independence of audit committee members? Even a hotline or tipline is limited in effectiveness if action is not taken in a timely manner. Furthermore, the documentation of the investigation is critical to reaching a proper conclusion whether fraud occurred.

For this course, our focus will be more on transactional controls. First, we will start by reviewing the great-great-great-granddaddy of fraud and fraud schemes – the eponymous name in fraud.

II. Charles Ponzi

No doubt you have heard the name. You may also remember that a “Ponzi scheme” is an investment in which early investors are paid returns on investment from later investors’ funds. Do you know what Ponzi was selling? What was the investment opportunity he used to bilk so many people out of their money? According to a Ponzi biographer, Michael Zuckoff, a journalism professor at Boston University, Ponzi was selling international reply coupons (IRCs). An IRC is a form of voucher. Multiple countries accept them in exchange for local postage. Why was an IRC valuable a century ago? Jets did not exist. There was no air

mail. Sending a letter overseas was expensive and slow; Ponzi could not speed delivery, but he could make it less expensive.[1]

Zuckoff describes Ponzi's scheme in The *Boston Globe* from May 22, 2022. Simply stated, Ponzi could buy 66 IRCs in Rome, Italy for the equivalent of one United States dollar ($1.00). That same number of IRCs, Zuckoff writes, would cost Ponzi $3.30 in Boston. That means, someone would buy an IRC for $0.015 each and be able to send a letter to Italy saving nearly $3.30! Incidentally, as of February 2025, that is the equivalent of $32.09 (adjusted for inflation)! With traditional mail being the best way to communicate, especially over long distances, it is no wonder that Ponzi soon had thousands of people queued up to invest.

Zuckoff states in the piece that Ponzi's scheme was technically legal, but practically impossible. As with any pyramid scheme, the sheer weight was too much to bear the load.

However, the op-ed article was not just a way for Zuckoff to tout his biography of Ponzi. He had another reason for writing the op-ed.

III. New Ponzi opportunity?

The headline, or title, of Zuckoff's piece echoes what your author has wondered: Is cryptocurrency a Ponzi scheme? He writes, "Good times roll, until they don't. This might sound like the stratospheric rise and recent plunge in values of the digital money known as cryptocurrency."[2] Let us see how this might work.

An information technology wiz and a friend in finance are chatting over cocktails. Discussing various topics, cryptocurrencies (or simply "crypto") come up. They dream up a scheme to start a new cryptocurrency. They decide to call it *Talent*. Eventually, they deposit $10,000 each in exchange for 10,000 Talents each. Away they go.[3] Investors see a new crypto on the market, and pounce to get in early—just like when Bitcoin initially sold for a fraction of a penny each.[4] Limiting the number of Talents to one billion, the competition picks up. The per unit price increases to $100, then $1,000, and peaks near $10,000 *per Talent!* Is this a scam?

As Zuckoff states, "Crypto believers reject the accusation by citing the relative transparency of the currencies' methods and the absence of deception. Detractors say the lack of underlying assets or government backing qualifies crypto for the Ponzi duck test. That is, if it walks, swims, and quacks like a duck, it's probably a duck."[5]

Discussion questions:

Do you invest in any cryptocurrency? Why or why not?
Do you believe crypto has a viable future for broad investment opportunities?

---

1 For more information, go to www.investopedia.com/terms/international-reply-coupon-irc.asp.

2 Zuckoff, Michael, *Is cryptocurrency a Ponzi Scheme?* The Boston *Globe* May 24, 2022, Vol. 301 No. 144, page A11. Accessed 24 May 2022.

3 We will not get into all the details of starting up a new crypto, that is not our focus here.

4 Edwards, John, reviewed by Julius Mansa, fact checked by Susanne Kvilhaug. *Bitcoin's Price History,* (2022, July 2) Retrieved from www.investopedia.com/cryptocurrency/bitcoin on 5 October 2022.

5 Zuckoff. *Is cryptocurrency a Ponzi Scheme?* The *Boston Globe*.

Shortly after the first draft of this chapter, the sudden collapse of FTX occurred. Michael Zuckoff appeared to be psychic. The allegations were that FTX founder Sam Bankman-Fried had been committing fraud. Bankman-Fried, often referred to by his initials SBF, claimed he did not intend to commit fraud. Typically, if someone takes money from someone as an "investment", that money is kept or used for other purposes to generate income. Banks accept money from account holders and invest the money in overnight investments to earn interest as well as lending it out to gain interest from the loan payments. It is alleged that Bankman-Fried spent the money on himself and on friends and family, and in addition donated to Democratic politicians. With some $1 billion unaccounted for as of the end of 2022, this appears to pass the "duck test" for fraud.

On December 11, 2022, Fox News Digital published an article titled "Future of the internet or a 'Ponzi scheme' – what exactly is Web3?" According to the article's author, "Web3 'offers a read/write/own version of the web, in which users have a financial stake in and more control over the web communities they belong to' by enabling users to own their data, according to the Harvard Business Review." [Hyperlink to the Review omitted.] Outside of confirming that we apparently do not own our data, a venture capitalist, Joe Lonsdale, was blunt. The article continues:

> "A lot of what people are calling Web3 was a Ponzi scheme, and it made no sense whatsoever," the Palantir co-founder previously told Fox News. "That said, the protocols to have decentralized ownership are very interesting."
>
> Decentralization, a key feature of blockchain, distributes the responsibilities of key internet functions such as server control, transaction confirmation, and time stamping to a network of users rather than traditional methods where all operations would be handled by one company or organization.[6]

Crypto may look like a Ponzi scheme, but that appearance may have been inadvertent. There is a flaw in Bitcoin and possibly other cryptocurrencies. There is a great deal of high level mathematics involved, and your humble author will spare you details as they are well beyond my math capabilities. It all comes down to how this electronic "currency" is stored.

Consider that someone bought one Bitcoin for $10.00 when it was a new thing. If you were buying a stock, you would send the $10.00, plus a commission, to the broker who in turn places the order. The printed (think *tangible*) stock certificates would be stored on the buyer's behalf in a secure room. Perhaps there would be a drawer with the buyer's account identification on it.

Bitcoin and all other cryptocurrencies are not tangible – you cannot hold a $10.00 Bitcoin. When one buys the Bitcoin for $10.00, a Data Miner must search for memory space to store that Bitcoin. The number one location as of this writing is in Tibet. There is a fee for this Data Miner's services, which may exceed $10.00. Nonetheless, it is stored with a "pointer", which is attached to the Bitcoin file that identifies it as belonging to the buyer with the password only the buyer knows.

However, Bitcoin was never meant to be widely used. The maximum file size is a mere one megabyte. Storage space is at a premium. Let us return to the stock purchase. What happens when the brokerage runs out of drawers in the secure room? Naturally, the brokerage must find space to build additional

---

[6] Raasch, Jon (2022, December 10) *Future of the internet or a "Ponzi scheme" – what exactly is Web3?* Retrieved from www.foxnews.com/tech/future-internet-ponzi-scheme-exactly-web3 on December 11, 2022.

drawers. What if there is no room in the brokerage's building? They must go to a new building. Bitcoin shot up to some $64,000 at one point because there was a rush on it. Those who purchased early saw the investment go up. Why did it go down? Because space was needed to store it. When someone sells $10,000 in Bitcoin to someone else, the Data Miner must change the pointer from the seller to the buyer. Both the buyer and the seller pay a fee to the Data Miner!

An article on SoFi.com provides additional information. This article states that "…Bitcoin miners are the ones who make sure everything is above board." This article, written by Samuel Becker, is focused on the mining fees, and it is the high mathematical abilities that seem to pay off big.

Mining fees: An overview and fee calculations

> Bitcoin mining is the process that validates and secures Bitcoin transactions and also [sic] creates new Bitcoin tokens (out of a total 21 billion bitcoins in existence). It's an intricate, resource-intensive process that utilizes high-powered computers to solve complex math problems.
>
> Once Bitcoin transactions are executed, they need to be verified. That means that they've been added to the public record and stored on the blockchain and verified to be accurate (not a duplicate transaction, for instance).
>
> Miners solve math problems (this is called proof of work) using Bitcoin mining software. The miner who does so unearths the next block on the blockchain which will store the transaction data and information. As a reward for doing so, miners receive Bitcoin or fees as a reward.
>
> Mining fees are like transaction fees you might get charged by merchants or banks. Another similar type of fee would be a foreign transaction fee, a fee that's incurred for transacting between two different currencies.
>
> Let's say you're using an exchange and want to send a friend, F, one bitcoin. Technically speaking, you're transferring X amount of Bitcoin from your address, or crypto wallet, to F's. Using your keys, you sign off on the transaction by specifying your bitcoin's address, F's address (or public key), and how much you want to send.
>
> A message is then sent to the network containing that information, and it reaches a mining node, where miners get to work validating and verifying it, and "mining" a new block on the blockchain. Before that change to the network takes place, you will be notified of the applicable mining fee for executing the transaction (which will depend in part on how busy the network is, and the size of the transaction).
>
> In effect, you'll have sent F one bitcoin, plus X% of a bitcoin (whatever the fee amounts to at the given time) as a mining, trade, or transaction fee.[7]

As mentioned above, the mathematics is extremely high level. In the end, Bitcoin and other cryptocurrencies were designed to be niche, but became too popular. As a result, it all appears to be a Ponzi scheme; but it is unintentional.

The FTX collapse was due in part to the design flaw in cryptocurrency and hastened by the misuse of customer funds.

---

[7] Becker, Samuel (2021, November 4). *Mining Fees: An Overview & Fee Calculations* Retrieved from www.sofi.com/learn/content/what-is-a-mining-fee/ on January 3, 2023. Hyperlinks within omitted.

Five Schemes That Shocked the World

Five Schemes That Shocked the World

Learning objectives

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

- Understand the magnitude of the largest fraud cases in recent years;
- Understand the perpetrator(s) might be one person, or large groups; and
- Recognize that some schemes could be easily spotted by a CPA.

I. Introduction

There are far too many cases of fraud to cover, even when limiting the scope to a single year. However, there are some cases that, like the attack on Pearl Harbor on December 7, 1941, will live in infamy.[1] What highlights the cases of corporate fraud is the scale and shear brazenness of the schemes and perpetrators. Not all schemes are pulled off by a single fraudster. Some, as we will see, are perpetrated by an entire organization!

What is corporate fraud? One writer stated, "Any kind of dishonest or illegal activities at the corporate level is Corporate Fraud… . Accounting Fraud is a subset of Corporate Fraud. In this case, a company's financial documents are altered to conceal the net loss, plummeting sales, or slow revenue. These are done to represent the organization as more profitable to potential buyers or investors."[2] Author Janet Brown's list is presented in the next section.

II. Five cases, plus

A. Capital One credit card data breach

Capital One presents a timeline on their website. The company states, "On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products."[3] The hacker's name is Paige Thompson, a former employee of Amazon Web Services.[4]

Capital One reports on the page that no credit card numbers or any login credentials were compromised. However, the company does report that around 140,000 Social Security Numbers were obtained, along with some 80,000 linked bank account numbers. The company also reports that it settled a lawsuit on April 22, 2022.[5]

What was in it for the hacker? Social Security Numbers in the United States are the key to one's identity. Think of the number of organizations that require providing the number. With those numbers, and with linked bank accounts, the perpetrator could have either sold the information for a lot of money and/or hacked other sites and stolen identities.

---

1 It may interest the reader to know that President Franklin D. Roosevelt's original statement in his speech was that December 7, 1941, was a date that would live in *history*. However, the president scratched that word out and hand wrote *infamy* above.

2 Brown, Janet. *5 Corporate Fraud Cases that has shaken the Business World* [sic]. Retrieved September 22, 2022, from https://askcorran.com/corporate-fraud-cases/

3 From www.capitalone.com, "Information on the Capital One Cyber Incident" accessed October 10, 2022.

4 Brown, Janet. Ibid.

5 From www.capitalone.com. Ibid.

B. Trade secrets stolen by Huawei

In another case from 2019, the United States charged a telecom company named Huawei with several corporate and wire fraud schemes. (The Chinese government, also referred to as the Chinese Communist Party (CCP), essentially runs Huawei.) The initial charges were that Huawei lied to the U.S. about operating a business in Iran. But there were other problems – namely that Huawei allegedly stole telecommunication technology from T-Mobile. The reader may recall that the U.S. asked Canadian authorities to arrest Huawei's chief financial officer.[6]

Why are these charges important for us to consider? The CCP/Chinese government makes no secret of their desire to be the sole superpower. China is buying up property in the U.S., much of it farms, and conveniently close to certain facilities. If you work in an organization with certain sensitive trade and business processes, see also *secrets*, then be certain to employ strict controls on your data systems.

C. Overseas hijinks

There is a saying that one ought to go big or go home. Steinhoff International is a combination South African, German, and Dutch international retail holding company. The company is listed on both German and South African exchanges. It was originally founded in 1964 in Germany. The company operates furniture and household goods stores primarily. One finds these stores in Europe, Africa, Asia, Australia, New Zealand, and the U.S.

Steinhoff offices in Germany were first raided in November 2015. Some two years later, share prices plunged when word broke that the company may have overstated profits and assets by nearly $12 billion.[7] It was a small group of executives who perpetrated this scheme. It is important to note that this took place *before the Covid-19 pandemic*! Since lockdowns, many retailers have suffered. Many have gone away completely, while some others have tried to stay solvent with online purchase options.

D. Please, accept my child

Was there something in the water in 2019? Author Janet Brown lists the undergraduate admissions scandal as another scam that shook the business world. Recall the scheme. Parents of children who may not have been either academically or athletically gifted used bribes to get their child or children into noteworthy institutions. These illegal transactions were between the parent(s) and an athletic coach in low profile sports.

One U.S. attorney prosecuting the case said, "The real victims, in this case, are the hardworking students." That is to say, the students whose parent(s) bribed a coach for a so-called athletic scholarship admission, pushed aside another student who may have actually been a better fit for the school and the team.[8]

E. Medicare fraud

What happens when the government provides a benefits program that grows to such size as to become nearly unauditable? Fraud, of course.

---

6 Brown, Janet. Ibid.

7 Brown, Janet. Ibid. Also "Inside the Steinhoff saga, one of the biggest cases of corporate fraud in South African business history" CNBC Africa. 28 June 2018. Retrieved October 10, 2022.

8 Brown, Janet. Ibid.

In this case, author Janet Brown writes, “At least two-dozen doctors and a few professionals from the medical equipment manufacturing firms were involved in [a $1 billion scheme].” The allegations are these doctors prescribed neck, knee, or back braces that were completely unnecessary for hundreds or thousands of elderly patients. The transactions were processed through call centers in the Philippines and Latin America. [9]

One can only imagine how many claims are processed by Medicare each day. The question for us is, how could an auditor who is not a medical professional assess whether something may be off? Let us gather some information.

First, the average doctor has between 1,900 and 2,500 patients. That is per physician – not the overall practice with two or more doctors.

Next, we need to determine how many patients are in an area. Your author chose to gather data on Fairfax County, Virginia, which is just outside Washington, D.C. According to the U.S. Census Bureau, the estimated population on July 1, 2021, was 1,139,720 people, of which 14.5 percent were aged 65 and over. That means around 165,300 people would fall into the pool.

The next part is much harder to assess. According to the website WebMD, “More than 50% of people over the age of 65 have some level of joint pain.”[10] The question is whether a brace of some kind is needed. Perhaps the reader may speak to their physician to get a handle on the numbers. For the sake of our example, let us assume that 40 percent of the patients age 65 and older require some sort of brace. That means that of the 165,300 patients in Fairfax County, some 66,120 would be prescribed a brace. If the average geriatrician has 2,200 patients, we expect somewhere around 880 would have a prescription brace per physician. We further expect there are about 75 physicians seeing patients.

The last wildcard in the deck for our analysis is specialty. How often does one hear from a friend or family member about a doctor that seemed to do a wonderful job with – insert issue here. Your author has two doctors that he could recommend for the right issue. This “specialist” may naturally prescribe more than the expected average. It is also possible that the specialist may use more diet and massage therapy than braces.

What was the likely undoing of the scam above? Money laundering. International shell companies and the purchase of luxury items such as yachts, villas, and exotic cars in the U.S. raised warning flags.[11]

F. One for the road

The U.S. Department of Justice (DOJ) won a conviction in 2022 of a Pennsylvania man and woman in another medical scheme. This one was to pay and receive kickbacks in exchange for the referral of prescription medications. Per the DOJ website, Dr. Steven J. Valentino, 65, of Haverford, and Michele Miller, 53, of Swarthmore, the office manager, participated in an incentivized prescribing scheme. It involved federal workers and Medicare beneficiaries. Valentino and Miller received kickbacks for referring, ordering, and arranging for medications to be filled by a pharmacy in Houston. The DOJ provided evidence that between May 2013 and July 2017, the pharmacy billed the Department of Labor Office of

---

9 Brown, Janet. Ibid.

10 Jordan, Michele; medically reviewed by Smith, MD, Michael W. March 29, 2021. *Joint Pain Isn’t Inevitable With Age*. Retrieved from www.webmd.com October 10, 2022

11 Brown, Janet. Ibid.

Workers' Compensation Program and Medicare about $2.5 million and was paid around $1.1 million for prescriptions referred, ordered, and arranged by Valentino and Miller in exchange for illegal health care kickbacks.[12]

There are at least two persons, maybe more, who might have uncovered this scheme. The first is the auditor of the pharmacy in Houston. When reviewing the customer list, the auditor would notice that a customer was in the Philadelphia area. Is this strange? Perhaps not. Were the medications being prescribed strange, given that the DOJ claimed some were "expensive compound medications."[13] If this pharmacy specialized in such medications, then perhaps it made sense. The second possibility on this side of the transaction is how the pharmacy recorded the kickbacks. Was there a "bonus pool" that was set aside? Were there "rebates" on prescriptions, or even "incentives" for "volume ordering"?

The second auditor is the one performing for the medical practice. What if there was no audit required – just a tax return? This would be the best way for perpetrators to hide their activity. No payment goes to the practice, though it may be shown as a "rebate" or "incentive." The benefit is that the transaction matches on both sides. The pharmacy pays an incentive, and the medical practitioner receives an incentive, or any other banal terminology. Professional skepticism goes a long way in uncovering fraud. Every flag ought to be heeded.

The DOJ does not reveal how the scheme was uncovered in its press release. However, the Internal Revenue Service (IRS) and U.S. Treasury do use techniques to track odd transactions, especially in search of money laundering schemes.

Discussion question:

Considering these scams above, what controls or procedures can you think of that would detect, if not prevent, such schemes from occurring?

One tool employed by the IRS is Information Returns Processing (IRP) System. It is simple. The IRS matches the information sent by employers and other third parties, such as financial institutions, to the information provided by taxpayers, for instance, on a taxpayer's W-2, 1099, and Schedule K-1. The IRS receives the information and checks the related Form 1040 for the individual's reporting of the income amounts. Your humble author once had a taxpayer receive a K-1 for a limited partnership that held commercial property. For years, the property in question yielded a loss, which the partners were able to use to lower taxable income. However, all those losses created negative basis, and when the building was sold, created a very positive *gain*. One partner, a medical doctor, asked us to change the return! He did not believe he should pay taxes on the gain. Naturally, we refused. If he failed to report the income properly, he would be subject to severe penalties. We never heard what this fellow did. But, if the IRS compared the information, he was going to get a visit.[14]

Simple mistakes are one thing. Cheating is something else. The IRS also uses certain filters to prevent fraudulent refunds for earned income tax credits (EITC). It is believed that the IRS tracks information from other sources to assess whether someone has more money than they are reporting. For example, the

---

12 Doctor and Office Manager Convicted for Health Care Kickback Conspiracy. Retrieved from https://www.justice.gov/opa/pr/doctor-and-office-manager... September 22, 2022

13 Ibid.

14 *How the IRS Catches Tax Cheats and Liars*. Retrieved from Investopedia at www.investopedia.com/articles/personal-finance/041515/how-the-irs-catches-tax-cheats-and-liars/ on August 31, 2022.

IRS allegedly searches medical records, credit card transactions, along with other electronic information to find potential tax cheats. The advice is to be very careful about what you post online.[15]

What type of post on Facebook or Twitter may be problematic for tax cheats? Trips that cost a lot, such as tours of Europe, Africa, even around the United States and Canada may lead an IRS agent to question whether all income has been reported. The IRS has said little to nothing about this technique. It is not believed that this alone would trigger an audit. There is a federal law called the Electronic Communications Privacy Act that permits federal law enforcement to view social media without a warrant along with emails stored more than 180 days. This data must be deemed relevant to an investigation. Those emails, by the way, are considered *abandoned*![16] Your author is curious about the Fifth Amendment to the U.S. Constitution that grants the right not to incriminate oneself. While not an attorney, it seems to your humble author that the right is surrendered by posting pictures and messages on the Internet.

Discussion question:

If you are in public accounting, will you mention this to your clients? If so, will you do so for their benefit, your protection, or both?

Naturally, we must include whistle-blowers that report to the IRS. The IRS hears from disgruntled employees and former spouses (even significant others) with reports of unreported income. Lest we forget, the IRS does pay rewards. Whether for revenge or a sense of "doing the right thing", the mandatory reward is from 15 to 30 percent of the collected amount over $2 million in tax, interest, and penalties. For an individual, the collection must be over $200,000. (Check the IRS website for changes in these amounts.) The IRS does have discretion for a reward of 15 percent on amounts up to $10 million collected.[17]

One final note on this subject. In October 2021, the U.S. House of Representatives and the Biden administration was pushing for *more reporting* by banks. According to an editorial in the Boston *Herald*, "The Biden administration has proposed requiring banks to report aggregate inflows and outflows of bank accounts to the IRS, in instances where bank accounts have flows exceeding $600."[18] The Democratic lawmakers had proposed to raise the threshold to $10,000 and to exempt regular wages'/salaries' deposits. It is unclear whether rent, mortgage, escrow, and other monthly expenses would have been exempted.

The editorial board wrapped up their argument writing:

> There is no real need to flag accounts – there is already a legal provision to do so, and it's been around since 1970. It's called the Currency and Foreign Transactions Reporting Act of 1970 (a.k.a. the "Bank Secrecy Act"), which requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, it requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000, and to report suspicious activity that might signify money

---

15 Ibid.
16 Ibid.
17 Ibid.
18 "Editorial: IRS, banks already work to catch tax cheats" Boston *Herald* editorial staff. (2021, October 13). Retrieved from www.bostonherald.com/2021/10/13/editorial-irs-banks-already-work-to-catch-tax-cheats/ on August 13, 2022.

laundering, tax evasion or other criminal activities. So the tax cheats? They've got an Act for that.[19] [sic]

It is possible that we will see this idea return more than a few times.

G. And another thing…

We cannot move forward without covering Theranos, Inc. This company was a medical testing device maker. Well, it was supposed to be. Here is a brief history of a $9 billion scheme.

The year is 2003 and 19-year-old Elizabeth Holmes is a freshman at Stanford University. Ms. Holmes believed that she could make a collection pen akin to how a diabetes patient tests blood sugar levels. Patients would not have to fill multiple tubes to test for various markers. Her company would develop a "mini-laboratory device" that Ms. Holmes called "Edison."[20]

Ms. Holmes quit Stanford to start Theranos. She used the remaining money her parents saved for her education to fund the company. She convinced one of her professors, Channing Robertson, to be a board member. Robertson connected Ms. Holmes with venture capitalists to provide additional funding. Keep in mind, there is no actual working device – just an idea, a theory. By the end of 2004, she had raised $6 million.[21]

Ms. Holmes' pitch was intoxicating. She perceived herself as a new Steve Jobs. Ms. Holmes "secured wealthy investors such as Henry Kissinger, Betsy DeVos, and Rupert Murdoch."[22] You may be aware of the adage that the devil is in the details. By 2014, Ms. Holmes' explanation of her testing technology started to garner more attention, even though the Food and Drug Administration (FDA) approved the first test.[23] Meanwhile, she had buy-in from her chief financial officer (CFO), Ramesh "Sunny" Balwani, who had joined the company in 2009. Mr. Balwani had no experience with either biomedicine or a technology start-up. "Employees quickly realized he did not understand the processes and technologies in the lab. Due to his fiery temper, Balwani quickly became known in the company as an 'enforcer'. Holmes hid the fact that she was in a relationship with Balwani from staff and the board."[24]

III. Summary

The schemes and scams we reviewed are some big deals that impacted people in ways that cannot be easily measured. The Capital One breach could have been worse. Huawei stealing trade secrets and violating patents harms trade and discourages improved processes and products. We saw in other instances above that an alert CPA or CPA candidate could have raised a warning with little more than a raised eyebrow. "Who is getting this [bonus/payment/incentive]?"

In the next chapter we look at the various groups of fraud schemes and the scams within the groups. Our goal is to see which controls ought to be in place to stop any fraud scheme quickly.

---

19 Ibid.

20 ____, (2022, November 21). *Elizabeth Holmes and the Theranos Case: History of a Fraud Scandal* Retrieved. from www.integrityline.com/expertise/blog/elizabeth-holmes-theranos/ on December 9, 2022.

21 Ibid.

22 Honaker, Brigette, (2022). *Theranos Scandal Timeline: How Elizabeth Holmes Built a $9 Billion Fraud.* Retrieved from www.topclassactions.com/lawsuit-settlements/prescription/theranos-scandal-timeline... on December 9, 2022.

23 Ibid.

24 Ibid, ___, *History*.

Groups of Schemes and Scams

Groups of Schemes and Scams

Learning objectives

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

- Understand the difference between a *scheme* and a *scam*;
- Comprehend the overall types of schemes and scams; and
- Realize that most perpetrators lack any sense of honesty.

I. Background

To better understand the various ways people can steal, we are going to start with two important definitions. Your author is a great believer in defining terms to ensure that understanding is maximized. There is an important distinction between *fraud* and *scam*, though some folks use the terms interchangeably. For us, we will be quite clear. You may recall in the eight-hour course CFVV or the four-hour course DRF4, we defined fraud and negligence. We will provide the former but from a different dictionary, and this time, the latter will be for the word *scam*.

A. Fraud, noun

1. Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage

For the prerequisite course(s), the definition was via The American Heritage Dictionary. In this course, to add some varying perspective, this time we are using the Random House Unabridged Dictionary. The first definition includes all the words one expects. However, if you refer to the earlier course material, American Heritage includes in the first definition the word “deliberately.” One may argue that Random House covers the intent via the word “perpetrated.” Random House goes so far as to provide the motivation, namely “for profit or to gain some unfair or dishonest advantage.” Curiously, both dictionaries have virtually the same second definition.

2. A particular instance of such deceit or trickery

Random House adds two examples, mail fraud [sic] and election frauds. Mail fraud, also referred to at times as mail and wire fraud, is a federal offense. If one is enticed to send money or other items of value through the United States Postal Service, or by wire transfer, it literally does become a federal case. This definition is pointing to instances of deceit and/or trickery leading off the first definition. As for election frauds, it is possible even likely that some have occurred. However, this area is not our concern in this course.

The next two definitions are closely related to the second.

3. Any deception, trickery, or humbug

Aside from the obvious connection to Scrooge, Random House provides an example, “That diet book is a fraud and a waste of time.”

4. A person who makes deceitful pretenses; sham; poseur[1]

The fourth definition points to the perpetrator, the one we often refer to as the fraudster. These are the people who we want to stop. And we will be reviewing the schemes and scams they pull for their ill-gotten gains.

B. Scam, noun; verb (*used with object*), scammed, scamming

1. (Noun) A confidence game or other fraudulent scheme, especially for making a quick profit; swindle

Let us be sure to factor in the key word here – *confidence*. You may be aware of the term, but you may also know it in its truncated form – con game, con artist, and/or con man. The perpetrator of this fraudulent scheme is likely looking for quick cash. It could be a few hundred dollars, or it could be thousands of dollars. The perpetrator gains the victim's confidence, making the victim believe they have found an advocate, a friend, or even a lover. The problem is that as soon as the perpetrator has the money, they go away. Any online connections are broken, profiles deleted, and any pictures were likely faked. And if the perpetrator used a phishing tactic to make contact, the perpetrator could be anywhere in the world.

These people are heartless and breathtakingly skilled at making their target believe they are who and what they say they are. They are "a senior member of the fraud prevention team." They could be "a United States military member trying to get home for a family member's wedding or funeral." They may really want to buy the lawnmower you have for sale, but they need you to have a PayPal account. Or they want to help you with your transaction, "but I need you to download a software so I can help you set up the account."

2. (Verb) To cheat or defraud with a scam[2]

While simple enough, the definition of scam provides the primary difference in what we will explore in this course. Fraud schemes are of long-term duration while scams tend to be short-lived. As you learned in the prerequisite course work, it is not unusual for fraud schemes to be active for well over a year before detection. There are some schemes that last a decade or more before being uncovered!

Two movies:

Your author recommends two movies to see schemes and scams in action. The first is the award winning *The Sting* (1973) starring Paul Newman and Robert Redford. Be warned that the story takes place in the 1930s, and the language used in the movie is true to the period regarding race. This movie demonstrates two scams – a quick hit to steal money without the victim knowing until it is too late, and "the big con" where the stakes are much higher, requiring a lot of set up.

The second is *Matchstick Men* (2003) starring Nicolas Cage. This movie focuses on Cage and his con artist partner. The critical line is spoken by Cage's character when questioned about taking people's money. Cage says, "I didn't take their money. They gave it to me."

---

1 Based on The Random House Dictionary. "Fraud." Dictionary.com; *The Random House Unabridged Dictionary* © 2022 Random House, Inc. Retrieved from www.dictionary.com/browse/fraud on October 18, 2022.

2 Ibid, "Scam."

Discussion question:

How do you feel about how Cage's character exonerates himself? Is it not true that the victims would not have "given him their money" if he did not fraudulently entice them?

What we also glean from these definitions is the sense of time, or the anticipated timeframes for the action. A fraud scheme is set up to syphon money over a long period of time. As we saw in the prerequisite course(s), a fraud scheme may not be detected for a year or more. Conversely, a scam is designed to get money quickly and the perpetrator(s) disappear. Carefully, see also deviously, planned scams may not be discovered for days or weeks after the money is turned over. This gives scammers time to get away from the area.

Both fraudsters and scammers seek the most amount of money possible in the circumstances. A long-running fraud may take hundreds or thousands of dollars at a time. The key is that the amount of money does not draw attention to the scheme. This is the long game. Scammers want enough money to live on for a while because each time they contact a mark, there is a chance of discovery.

II. Fraud schemes – Types

There are three types of fraud schemes, or one might say three groups of fraud schemes. They are Corruption, Asset Misappropriation, and Financial Statement Fraud. The largest of the three is asset misappropriation. The Association of Certified Fraud Examiners (ACFE) breaks these down into subgroups.

There are four subgroups of corruption schemes. The ACFE labels these Conflicts of Interest, Bribery, Illegal Gratuities, and Economic Extortion. Of the three main groups, this family of fraud schemes is the smallest. That is not to say that they are not as harmful to victims.

There are two subgroups the ACFE defines under financial statement fraud. Both subgroups deal with Net Worth/Net Income. The only difference between the two subgroups is whether the net worth and/or net income is overstated or understated.

The largest group, asset misappropriation, also has more subgroups than the other two groups. The ACFE breaks out two large subgroups of asset misappropriation. They are Cash and Inventory and All Other Assets. Under Cash, the ACFE breaks down the subgroup further with Theft of Cash on Hand, Theft of Cash Receipts, and the big one, Fraudulent Disbursements. Under Inventory and All Other Assets, the ACFE has two more subgroups, which are Misuse and Larceny, the latter having additional schemes listed.

You can find a nice graphic on this in Figure 3, on page 10 of the ACFE's *Occupational Fraud 2022: A Report to the Nations*.

III. Scams – Types

There is a variety of scams. Scams are initiated in two broad ways – in-person communication and phishing. The in-person scam may be initiated on the phone or by someone ringing your doorbell. It is also possible the scammer is posing as a legitimate street vendor. Because of the Internet, however, scammers have several tactics.

The first general type of scam plays on emotion, primarily love and friendship. The type is a phony government official or someone claiming to be royalty in another country. A third type is the alleged need to front money to enable you to claim prize money or product. Lastly, in a category all by itself, a type that is on the rise in the wake of Covid, is employment opportunity.

Discussion question:

Do you believe that you are too savvy to fall victim to a scammer?

Consider that with advances in software, scammers can recreate websites and emails that closely resemble their actual counterparts. It is too easy to use the Microsoft Snipping Tool to lift logos, addresses, and other indicia to create convincing fakes.

IV. Final thoughts

Whether a fraudster or scammer, perpetrators can easily convince the mark, the target, and let us simply say the victim, whether a company, family, or individual, that the fraudster/scammer is honest and trustworthy. Imagine someone with the acting skills of any of the best actors on stage or screen, but with next to zero integrity. It is someone so selfish and sneaky, they have their victims completely hoodwinked. My mom used to say, “You never know about people.” The statement could relate to anything. Perhaps by the time you finish this course, you, dear reader, may not want to trust anyone. That is not the goal of this course. The goal of this course is to present the schemes and scams and the means we can employ to mitigate the risk of loss.

In the next chapter, we will dive into the schemes and scams within the various types we developed above.

Schemes and Scams

Schemes and Scams

Learning objectives

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

- Understand the general categories of fraud schemes;
- Understand various schemes within those categories; and
- Realize that schemes may be perpetrated in more than one form.

I. Introduction

We have our foundation, now we are going to build out our groups of fraud schemes and scams. We are using the ACFE's "The Fraud Tree" as our guide for the discussion.[1]

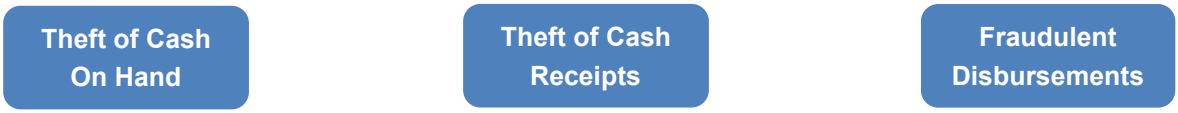
We discuss the details of the schemes and scams in this chapter, and address controls to detect the schemes in the next chapter. Vigilance and skepticism are one's best defense against scams.

II. Asset misappropriation

The ACFE identifies two categories of asset misappropriation:

Under cash there are three subsets of schemes. Two of the three are closely related: cash on hand theft and the theft of cash receipts. The third subset is fraudulent disbursements. Under all three of those subsets are numerous schemes listed.

A. Cash



The outright **theft of cash on hand** is simple – someone with access to the petty cash, cash drawer and/or cash in the coffee and snack fund pilfers the cash. A simple deterrent is locking the receptacle and/or placing the receptacle in view of a camera. The theft of cash receipts, however, goes much deeper.

1. Theft of cash receipts: Cash larceny

This side is straight forward – snatching cash from the so-called till or from colleagues when they are not looking and alert. The amount of cash taken may be small, between $5 and $20 if purses or wallets are

[1] See, the ACFE's *Report to the Nations* (2022), Fig. 3, p. 10, (2020) Fig. 3, p. 11.

left out in the open. This is a quick hit and is one form of “gateway fraud,” discussed in the prerequisite course(s). A more persistent theft scheme, and a one-time larceny morphs into all out embezzlement.

2. Theft of cash receipts: Skimming (embezzlement)

There are another three sub-sub-sets of skimming. Cash may be skimmed from **sales** by either pilfering cash in the drawer or never inputting the sale into the system. The customer believes the transaction is complete and the company never knows it takes place. This is where sales are either unrecorded or understated. These types of schemes were prevalent in retail stores before the high usage of credit and debit cards and companies opting to be “cash free” to mitigate theft, whether by an insider as just described or someone who robs the store.

Closely related to skimming sales is skimming cash via fake **refunds**. This was another prevalent scheme, and still is. Have you ever been contacted by a vendor whether brick and mortar store or online vendor and asked how your experience was with the return and refund process? In the late 1980s and early 1990s, stores required customers making a return with cash back to complete a refund form that included name, address, and telephone number. Someone would gather these forms and randomly select a sample to contact to ensure first that the transaction did take place, and that the customer’s experience was positive enough to maintain their patronage. There may be a few **other** types of fraud schemes, but with the use of cash diminishing, these others would be more high-tech.

The third sub-sub-set of skimming is from **receivables**. Following on the fake refunds, phony write-offs of receivables, which ties to financial statement fraud, is one that may include an accomplice. A vendor is owed money from a buyer, but someone in accounts receivable (perhaps even an accounting manager or controller) at the vendor colludes with someone in accounts payable at the buyer. The plan is to “write-off” the receivable, which may mimic the fake refund scheme, and have the cash to pay the receivable go to the accounts receivable perpetrator. This person then disburses part of the cash to their colleague in fraud. Unless someone notices the payoff or sees a pattern of an inordinate number of write-offs, this scheme can last a while.

There are two other types within this sub-sub-set. They are lapping schemes and unconcealed. The latter is exactly that – the perpetrator(s) does nothing to hide the theft. Someone stole cash, but it is not known who. Management sends out a forceful email and expresses disappointment. The lapping scheme takes work, and like a Ponzi scheme, is likely to fail under the weight of having to cover payments. Cash is received to pay Invoice 10001 but is pocketed. Cash to pay Invoice 10002 is applied to clear 10001. Excess is applied elsewhere while a shortage carries forward.

3. Fraudulent disbursements

When it comes to asset misappropriation, this is the jackpot. Some of these schemes are related to others we have already covered, and you will see by their names how they tie together. To make it easier to follow, we will break these down one sub-set at a time.

Billing schemes

The first sub-group is billing schemes. The top dog in this group is one that takes planning and some money – the *shell company*. The shell company must appear to be legitimate to the accounts payable system. That means it is likely going to have a record with a state’s Secretary of State’s corporate registrations website. There will be some identification number, and likely will be an entity that does not require a Form 1099 to be sent by the victim organization. Invoices will be for something reasonable and

not easily questioned. A shell company is not really a going concern. It is a name, address, telephone number, and perhaps a website, and that is all it is. The money to pay the invoice from the shell company goes to a bank account in the company's name. Be wary of a bank account that is offshore. Keep in mind that the victim organization's own employee may set up a shell company.

Conversely, the *non-accomplice vendor* is a second victim. In this case, an invoice is sent by the vendor believing the charges are correct. The easiest example of this is *timesheet fraud*. Both the vendor and the buyer can catch this scheme with vigilance. Literally, observing whether the vendor's personnel are where they are supposed to be, noting the times when the person is not there. A quick check of the hours billed may prove revealing.

The last of the billing schemes to cover is billing for *personal purchases*. This may happen when someone is traveling for business but includes costs for personal items or excursions.

Payroll schemes

Payroll schemes take longer to detect than other schemes. The ACFE's Reports to the Nations over the last decade have consistently shown that these schemes take at least six months longer to detect. One logical reason is that payroll is generally considered highly sensitive. Inquiring can open the inquirer to push back. We believe our internal controls work. We may have tested them and found them to be designed and operating effectively. Still, these schemes occur often and may be present in your organization right now!

The three schemes are tried and true: ghost employees, falsified wages, and commission schemes.

A *ghost employee* is payroll disbursed to someone who is not actually an employee. It is one of the easiest schemes to detect – provided the Human Resources (HR) department will cooperate with the auditors or other internal audit or examining personnel. HR is very particular in keeping employee information from eyes the HR department believes has no reasonable need to know. We will cover the controls to detect and prevent fraud schemes in the next chapter.

Above we discussed a non-accomplice vendor who invoiced a company for labor that never took place. For the unsuspecting vendor, this is a *falsified wages* scheme. Of course, wages hints at an hourly employee. There is also a salaried employee version of this scheme. Suppose a consultant is supposed to report to a client company. The client company is large with a lot of floor space broken up by offices and cubicles. The consultant's space is out of the way of the main work areas to limit the exposure of proprietary information the consultant has no reason to hear and see. The door is open for the consultant to claim hours when the consultant is not even there.

Closely tied to the timesheet (falsified wages) scheme is the *falsified commission* scheme. The one takes a little more than a fake timesheet to pull off. This is also a sales/revenue fraud. When your author entered the workforce, the first job was selling men's suits at a prominent retailer of the time. Commissions were not for me because I was part time. The three full timers, however, needed those commissions. Fortunately, no one ever asked me to falsify the sales record. Suits are one thing, but can you imagine trying to boost commission on other items, such as computers, cars, or other items? If commission is to be paid, something must be sold.

Expense reimbursement schemes
This is a set of somewhat easier schemes to pull off. An organization that has personnel with travel and other reimbursable expenses is going to become a victim of all of these: mischaracterized expenses, overstated expenses, fictitious expenses, and/or multiple reimbursements.

Organizations will permit their personnel to be reimbursed for business expenses. The expenses may be for mileage, meals, hotels, airfare, lodging, and other professional expenses (such as continuing professional education courses for continuing education credit). The organization will not typically pay for personal expenses. Some are tempted to *mischaracterize expenses* to be paid back. In economically rough times, certainly if the employee has a significant financial burden, this one is easy.

The first scheme ties closely to the next two schemes. *Overstated expenses* are those that were incurred; however, the amount is inflated. *Fictitious expenses* were not incurred. The latter scheme may also be perpetrated by re-using receipts and invoices and doctoring the documents, which we call *multiple reimbursements*. This last one can also include paying two different entities for the same expense. For example, a person travels and submits a receipt for dinner. Subsequently, another person travels and submits the same receipt, though it may have been electronically modified. The persons split the proceeds of the duplicate reimbursement payment.

Check and payment tampering
The first part of this category – check tampering – is obsolete. The use of checks has been greatly reduced with electronic fund transfers (EFT) through automated clearing house (ACH). However, this does lead to the second part of payment tampering. In either case, someone either alters a check (payee or amount) or alters the file prior to submission. The one other item that can be altered is the destination account information. Changing both the routing number and the account number may be possible, depending on the controls in place for access and changes. This captures the four schemes under this category, *forged maker*, *forged endorsement*, *altered payee*, and *authorized maker*.

Register disbursements
We touched upon *false voids* and *false refunds* above. There is nothing to add here.

B. Inventory and all other assets

The sub-category is **misuse** of the inventory and other assets. For example, a company-owned vehicle for business purposes only (such as delivery) is used for someone to run errands. Perhaps the easiest “other asset” to misuse is the organization’s Internet connection. Many employers do permit limited use to check email or send an email that is critical. Many employers also permit limited use on “Cyber Monday” for holiday shopping. The misuse of phones was an issue decades ago, but with cell phones everywhere, folks can glance at it for important messages and calls.

Discussion question:

Does your organization permit limited use of certain company assets? If so, do you believe that this is helpful? If not, do you believe it would benefit morale and ultimately, productivity?

The second category is **larceny** of the inventory and other assets. The fourth scheme listed by the ACFE is *unconcealed larceny* which we noted above means that we know something was stolen. We may even know exactly what was stolen. We will leave that be.

The first of the schemes is using *asset requisitions and transfer* to move the asset. For example, in a chain of retail stores, an employee in Store One colludes with an employee in Store Two. The first employee completes an inventory transfer for an item. The item is "shipped." The employee in the second store "receives" the item, though it never actually arrives.

The second is closely related to the first, but it is related to *false sales and shipping.* Change the second employee above from Store Two to a coconspirator posing as a customer. The problem with this is "payment." With phony requisitions and transfers, no money is involved. False sales, however, create an expectation of revenue. This scheme may take place more between a vendor and buyer. A buyer believes a dozen items have been delivered, but only ten are. The false sales and shipping information is more true than false, but the difference in the amount paid for 12 with only 10 delivered is the spoils of the coconspirators. Similar schemes have taken place in recent years! These schemes tie to the third in the list, *purchasing and receiving schemes*.

III. Financial statement fraud

This is the second largest group of fraud schemes in the ACFE's "Fraud Tree." As noted in the prerequisite course(s) and in this one, all fraud schemes end up somewhere on the financial statements. When we discuss financial statement fraud, we are referring to deliberate alterations of the financial statements, typically through journal entries, to alter the perception of the financial condition of the entity.

Net Worth/Net Income Overstatements	Net Worth/Net Income Understatements

The ACFE lists five schemes under each. No surprise, they are identical, except for two sets, which are opposites.

The first of the schemes is **timing differences**. We know that timing differences occur, which is why we try to use accrual accounting to capture those differences. These schemes (keep in mind they can overstate or understate net worth and/or income) are deliberately using the timing differences to bend the truth. One of the easiest schemes is when an entity "pays" accounts payable but places the out-going envelopes in a drawer to be mailed days later. If you have a client who still uses checks for accounts payable, this could be an issue.

The next is the first of the opposites – **fictious** and/or **understated revenues**. The motives differ, depending on the schemer's intent. If higher revenue helps get a loan, lower revenue may help lower taxable income. There may be other motives, too. Any journal entry made directly to revenue and equity, without passing through the sales journal, ought to be examined.

The third set of schemes is also the second of the opposites. These two are **concealed** and/or **overstated liabilities and expenses**. Concealment makes sense, but why might an organization want to overstate liabilities and/or expenses? Perhaps the organization is applying for federal relief (think of the relief passed by Congress during the SARS-CoV-2/Covid-19 pandemic).

The last two sets are identical in each group, and they are **improper asset valuation** and **improper disclosures**. Auditors ought to catch the latter when reviewing the final financial statement for signature. Improper asset valuation ought to be caught during the interim or field work. This one comes in many

flavors. An allowance for doubtful accounts may be too low or too high. Inventory may have been prematurely written down or off, or could be at original value, but nearly obsolete.

IV. Corruption

The ACFE lists four general categories of corruption.

From left to right, the first two stand alone. **Illegal gratuities** are exactly what it says. Gratuities are common, and expected, in service industries. We "tip" our restaurant servers, Uber drivers, and others. It is expected. An illegal gratuity typically is associated with *quid pro quo*. The "tip" is actually a payment for anticipated benefits to follow.

Similarly, **economic extortion** is a threat to harm the organization in some manner unless something does or does not occur. "You'll buy your widgets from ACME Widgets, or else something bad may happen to your production line." Of course, this also happens between nations. One country threatens economic consequences unless another nation acts in a certain way.

Both types are a close cousin to item B below.

A. Conflicts of interest

The ACFE lists two types of schemes under this sub-group. Let us remember that the term "conflict of interest" is a slight misnomer. A buyer and a seller have an interest that conflicts with one another. The buyer wants to acquire something for as low a price as possible while the seller wants to sell for the highest price possible. A true conflict of interest is when a single party to the transaction has more to gain than in a typical transaction.

Continuing the buyer-seller situation above, suppose the seller is Joe and the buyer is Jane. Jane is interested in buying Joe's car. Jane says that she would like to have her mechanic check the car out before she commits to the purchase. Joe agrees and asks Jane if she knows anyone. Jane says she is going to look online and call someone. Joe suggests the auto repair shop about a mile away. Jane goes to the shop, asks if someone can check out the car, and a mechanic there says, "Sure. Where's the car?" Jane says to follow her.

What Jane does not know is that Joe had all his auto repair and maintenance done at this shop. The conflict of interest exists because Joe knows the mechanic is not going to call out inferior work on himself. Further, the mechanic is going to confirm the maintenance of the car is very good to excellent.

The two types of conflicts of interest the ACFE mention are **purchasing schemes** and **sales schemes**. These are two sides of a coin.

B. Bribery

Finally, we conclude our climb of the ACFE's "Fraud Tree" with two more schemes. **Invoice kickbacks** may be spawned through a *conflict of interest*. One example is the sales representative for the vendor is trying to improve commission income and performance reviews. The representative entices their

counterpart to agree to fake line items on an invoice. In exchange, the representative will send half the excess funds back to the buyer. This form of scheme may be pulled off even more easily with labor hours. The buyer "approves" the inflated timesheet and pockets money from the overpayment.

Another version of this first example is that the sales representative promises to send back a portion of the payment simply for the business. The buyer agrees, even if the goods or services might have been procured for less with another vendor.

Lastly, an old favorite when governments are involved, good old fashioned **bid rigging**. There are two main ways this classic is pulled off. The first is that specifications and requirements are tailored to fit one, and only one vendor. The chief of Smalltown Fire Department has convinced the town's board of selectpersons to acquire a new fire truck. It will cost the town $850,000. The chief wants a specific manufacturer to provide the truck, but a request for proposal must be available to all fire truck manufacturers. The chief reviews the specifications for a truck that would meet the town's needs on ACME Fire Apparatus's website. Sure enough, when the chief has the specifications ready, they meet to a tee the trucks ACME builds. The other companies cannot meet the specifications.

The second version is the inverse of the first. In this scenario, ACME sends its truck specifications to the chief and may offer "an incentive" if the chief tailors the specifications.

There may be other nuanced ways bids can be made such that only one company can meet the specifications and qualifications. In fact, if you are familiar with government contracting at the federal, state, and local levels, you may know that protests often follow a contract award, many times intimating something was wrong with the bid and proposal process.[2]

V. Bonus schemes

There are a few other schemes to mention. These come courtesy of i-Sight.com.

You may remember the members of the United States House of Representatives were caught in a large **check kiting** scheme. In the era of ACH/EFT, this scheme is falling off our radar. This occurs when a check is written when there are insufficient funds to cover the check. Back in the olden days, someone could write a check on the first of the month, place it in the mail, and it would not be received for three or four days. The payee would go to their bank and deposit the check. The check would then be sent to the check drafter's bank for the money to be moved. This might take another three to five days. But as i-Sight notes, "This type of fraud scheme is less common nowadays, with faster check clearing times."[3]

There was a time when I worked for a workers' compensation insurance company. The claims department had some wild tales. That brings us to **workers' compensation fraud**. There are several versions of this classic scheme. An employee may exaggerate an injury, disability, even invent injuries that never occurred or occurred outside work. In some states, workers' compensation payments are not taxed as income, or are taxed at lower rates. The fraud continues when the employee lies about their health to delay returning to work, even though they are fit to return.[4]

---

2 Ibid.

3 Lomer, Dawn (2017, March 17). *41 Types of Fraud and How to Detect and Prevent Them* Retrieved from www.i-sight.com/resoures/41-types-of-fraud-and-how-to-detect-and-prevent-them.html on September 23, 2022

4 Ibid. The article suggests seeing their article *31 Warning Signs of Workers' Compensation Fraud* at www.i-sight.com/?p=57945

That scheme ties to **health insurance fraud** which also can be perpetrated a couple of ways. The employee may conspire or collude with their health care provider to defraud the insurance company with false or inflated receipts. The employee could claim reimbursement for care never provided. Or the healthcare provider could pad the services provided to collect more money.

Another scheme that relates to the receipt of products is **product substitution**. In this scheme, whether the supplier acts on their own, or colludes with the purchaser's employee, inferior or counterfeit products or materials are shipped rather than those specified.

The new granddaddy of fraud is **data theft**! Hackers can grab all kinds of data, including any trade secrets, customer and contact lists, and the theft of personal identifying information (PII).[5]

Roundtrip transactions occur between two or among three or more organizations where there is no apparent business sense, purpose, or economic benefit. Common in money laundering schemes, these transactions serve to boost revenue, or to imitate and inflate growth.

We mentioned paying accounts payable and keeping the payments in a drawer above. The flip side of this is **bill and hold**. In this case, a sale is recorded, however the delivery is delayed. Transfer of ownership does not occur on the date the "transaction" is recorded.

Another scheme related to revenue inflation is one for **up-front fees**. Customers may have to pay certain fees immediately for the services or goods to be provided over a longer period. The organization may try to recognize all the revenue immediately – before the revenue has been earned – rather than over time as the revenue is earned per generally accepted accounting principles.[6]

VI. Bonus scheme insights

Doing the research for this course, your author found several shorter articles with much of the same information as the longer article and white papers used. This information ought to be mentioned. For example, vendor kickback schemes may not pay off in cash.

> Kickbacks can also include loans without interest, extravagant entertainment, free travel [sic] or gifts. Even the promise of future employment may be considered a kickback. In these situations, red flags can often include a lack of competitive bidding procedures within the company, poor supervision of purchasing, or management applying heavy pressure on employees to use a certain vendor.[7]

Above we discussed fraudulent expense reimbursement. We cannot leave this chapter without mentioning what may be the easiest internal control gap to fix, yet easily exploited: procurement credit cards (P-cards) and travel cards. P-cards are an extension of petty cash. However, without a strong policy and procedure, not to mention oversight, these cards can be a fraudster's dream come true. Continuing from the article quoted above:

---

5 Ibid.

6 ____. *Different Types Of Fraud Schemes.* Retrieved from www.financialcrimeacademy.org/different-types-of-fraud-schemes/ on September 23, 2002.

7 Vona, Leonard W. (Undated). *Five Common Fraud Schemes & How to Identify Them.* Retrieved from www.leonardvona.com/blog/five-common-fraud-schemes on September 23, 2022.

> Purchasing cards and travel cards are useful tools for paying travel expenses and automating supplier and vendor payments. These can eliminate unnecessary paperwork and cut down on administrative costs. There is, however, a temptation to take advantage of the system by using the system to purchase unnecessary items. For example, an employee might buy items for themselves on the card, pretending they are gifts for clients or research for work.[8]

With P-cards, be on the lookout for transactions that are close to the threshold that would eliminate the use of the card. Years ago, I was auditing my then employer's P-card and noted several instances of split transactions. One was for the purpose of concrete that was needed for the project. It cost just over $5,000. There were two charges: one for $2,999.00, and the other for the balance. The threshold for a purchase requisition to obtain a purchase order was, you guessed it – $3,000. Not only did I have a problem with the split transaction, given the nature of the project, concrete had to be ordered! It may have been that the concrete provider wanted quicker cash and the P-card provided it.

Also from your author's experience is workers' compensation procurement fraud. This means, the insurance company will require a roster of employees to be covered and the job codes. The codes relate to the type of work performed and each code has an associated risk. An office worker has less risk than someone working on a construction site. In this case, a client both understated the number of employees and misrepresented their labor code. Had anyone been hurt on the job and needed to claim workers' compensation, the consequences would have been severe. The company might have gone out of business.

There is one more thing before we turn attention to controls and procedures to prevent and detect fraud schemes. Whether you work in public accounting or in the private sector, are you aware of who in both the auditee organization and in their vendors and customers, not to mention banks, receives and provides audit confirmations? Remember that several schemes discussed in this chapter incorporate two or more parties who may work for different organizations. Consider these insights:

> Fraudulent audit confirmations can impact all types of accounts or transactions that are confirmed with third parties (sales, cash, accounts receivables, debt, liabilities, etc.). Schemes may involve collusion with third parties who receive the audit confirmations or may involve the company providing the auditors with false contact information (false mailing addresses, fax numbers, phone numbers, etc.) so that confirmations are diverted to co-conspirators involved in the scheme.[9]

Mailing confirmations certified may not be the answer. Asking your point of contact who is supposed to receive them may help (assuming the contact is not part of a scheme).

VII. Scams

As noted earlier, we are defining "schemes" as a fraud designed or intended to last a long period of time. A "scam" is typically a fraud that is meant to strike once, and payoff for the scammer. Many scams start with phishing. An email is sent, or contact is made via social media to the intended victim. We will review ten common scams. The foundation of this section is from *10 Common Fraud Schemes and How to Protect Your Money* from CentralBank.com. Note that they use "schemes", but we will use "scams" here.

---

8 Ibid.

9 Potnis, Neeta and Khanapurkar, Nitkin, (2009) *Sample listing of fraud schemes.* Retrieved from Deloitte Centre for Corporate Governance © 2009 Deloitte Touche Tohmatsu India Private Limited on September 23, 2022.

A. Romance

These scams can devastate someone. Not only is money lost, and the risk to other assets may exist, but a person may lose trust in people who can be trusted. These scams start with someone befriending the intended victim. The person is overseas, in the military, a member of royalty, wealthy widow or widower, or some other place in their life that is plausible. This is the first red flag. The next is that the person claims they are in love with the victim after a few exchanges. In the case of military, they may not be able to complete an EFT without the victim sending money. For “marriage”, well that is going to involve legal fees and visas. All these cost money that must be sent right away! (HUGE red flags!)

Of course, there are complications, and more and more money will be needed. They will keep their prey in their grasp for as long as possible. The best defense is to be aware of these scams and alert your family and friends. Your author receives five phishing emails a week!

B. Friendship

True friends are priceless. Like the romance scam above, this scam befriends the victim because of something in common; favorite teams, birthplace, wine, and anything else that creates a connection. After a few exchanges, the scammer writes, “I really appreciate your listening to my problems. Can I confide in you?” The baited hook is dangling before the fish. The scammer confides that a child needs surgery, or else the child will die! But it is all nonsense. The costs continue to increase. The first surgery went well, and the doctors believe the second will go just as well.

True friends are priceless; fake friends may cost a fortune. Be certain to check privacy settings on social media accounts.

C. Facebook friends

In this case, remove the “r” from “friends” and that is what you have. The scammer has hacked and hijacked one of your friend’s accounts. They ask for money for some reason. “We’ve known each other since high school!” If it were not for Facebook, it is likely there would be no contact whatsoever. You do not even go to reunions!

A few months before the first draft of this chapter, your author received a text message from a former sister-in-law. She was married to one of the brothers of my former wife. The text came out of the blue. We are still connected through social media, but other than an occasional “like” of a photo, there has been no communication for several years. (That is sad, but it is the way it goes. They are a great family.) However, your author was very suspicious of the message. I texted her husband, my former brother-in-law and alerted him that I suspected her Facebook page had been hijacked or her phone had been hacked. I never heard anything after that. The lesson: beware of these random contacts you have heard nothing from in years.

D. Distraught grandchildren

In this scam, the victim is contacted by a grandchild who claims to be in trouble. They could be in jail, the hospital, or “they need to get married” and do not want their parents to know. Quick hint that something is wrong is the third one. People have children out of wedlock in the 21st century all the time. Why would they not want the parents to know about being in the hospital? Who is carrying the health insurance? The kicker is that the money must be sent to them in a foreign country!

Your author *never* posts while on vacation. It is a means of keeping thieves away from my home. However, at least one trusted neighbor knows to watch the house, the local police know to watch the house, and family members know the destination and time frame. If your author calls for money, it is legitimate! Otherwise, hang up or block this scammer immediately.

E. Prince or government official

This person claims to have millions of dollars (or some equivalent in some foreign currency) but needs the victim's help to get through customs, pay taxes, or bribes to get the cash out of their country. The scammer offers an amount from their fortune if money is sent or worse, the victim provides their bank account information.

In recent years, a twist to this scam emerged with the caller claiming to be from the United States' Internal Revenue Service. The intended victim owes taxes but can clear the debt right now with gift cards or some other odd request. It is a scam.

F. Lottery or sweepstakes you never entered

Congratulations you won the Jamaican lottery! Not. The emailer states you only must pay taxes to move the money through customs. Then the customs collectors need more money. And the beat goes on. Of course, the lottery could be any country. But, the next scam might also get by, unless…

G. Customs clearance/advance fee

We discussed advance fee fraud schemes above. In those cases, the fees may be added to otherwise legitimate invoices. These scams are different. Again, it appears to be someone known to the intended victim. There is something of value your friend needs to get through US Customs or out of another country. They ask to have the fee sent to them, including what appears to be a very official looking email from Customs with the amount needed. There is one thing that these scams have in common, and we will mention it here: an inordinate amount of spelling errors!

Your author is writing in English, my first language. Word has auto-correct and suggestions. I cannot tell you how many times suggestions pop up while I write this course, memos, reports, or whatever else. Scammers are writing in a language other than their first, and their computers may not have the ability to make the auto-corrections in a language other than the local language. Furthermore, the scammer may not be fluent in the language and understand grammar and usage.

H. Internet sale

Your author experienced an attempt at this one when I was selling a riding mower I no longer needed. But, in that case, someone "in the U.S. Army" needed funds transferred to buy the mower for his son in another state. Of course, the scammer was overseas. Enough said. A riff on it is when a scammer sends $15,000 for a car the victim offers for $10,000. All the victim has to do is deposit the check and send the extra $5,000 back. Once the car is shipped and the extra cash wired, would you believe the check bounces?

I. Internet loan

Suppose you want to buy a car for $10,000, but you do not have a terrific credit score. You apply for a loan on a website that appears completely legitimate. When you receive the money, perhaps by check, there is a note that they want some money back "to show good faith and that you will repay the full loan."

Like the scam just above, the check bounces, and that "good faith money" paid is lost. That's all the scammer ever wanted. Even worse, the loan information provided allows the scammer to steal your identity.

Never do a loan online without vetting it completely. Speak to your banker.

J. Internet job

This scam is exploding in the post-Covid world. A job is offered as an assistant to an overseas business. All that is needed is for the mark (that is, intended target/victim) to open a bank account for them so they can send money for the mark to distribute to customers in the United States or other countries. Once opened, funds appear via wires, ACH/EFT, and/or checks. The victim is told where to send the money "as part of the job." So, what is the scam?

Shortly after these transactions are completed, the victim is informed that the funds were stolen! It is likely the informer is "law enforcement", perhaps Interpol or FBI. And the hook – the victim is told that the *victim* is responsible for the theft but can clear it all up by replacing the money. The money placed in the account was essentially "seed money" likely obtained from other successful scams.[10]

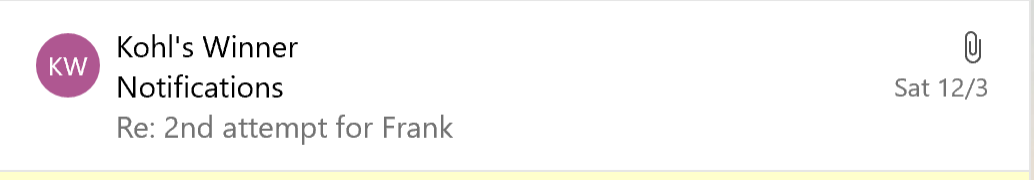
The article concludes with important information:

> Scammers hope you are too embarrassed to tell anyone that you fell for a scheme or too proud to admit you were tricked and keep sending money their way to show you were right all along. [That is, you were "right" that it was all "legitimate."] If you think you are being scammed check with someone you trust. A banker attorney can help you protect what you worked so hard to obtain.

VIII. Bonus scam information

A. The basic scam

The number one scam operating now is "confirmation" of a phony purchase or subscription renewal. Imagine what your author discovered in the email inbox.



We are not blaming Kohl's for this – their good name is being hijacked! What does the email look like when opened? Impressive…

[10] ____ (Undated). *10 Common Fraud Schemes and How to Protect Your Money*. Retrieved from www.centralbank.net/learning-center/common-fraud-schemes-and-how -to-protect-your-money on September 23, 2022.

To: FrankTT@aol.com Cc: FrankRF@aol.com

27.17 KB

Re: 2nd attempt for Frank

Who would not want this nice cookware? I want you to look in the upper left corner and look at the two email addresses. They are FAKE. Neither one comes remotely close to mine. Which “Frank” do they mean?

When you receive suspicious emails, you can right click on the sender to get details. Doing this, you will quickly see it is all utter nonsense. Turn the page.

KW

Kohl's Winner <info_nswVeQ548qg@news.ncgcypddscu.com>

12/3/2022 10:23 PM

That email address is a dead giveaway that this is bait.

Another high-paying scam is one where the mark believes that the “renewal” of Norton or some other product is bogus, and the mark wants to report the fraud. Gotcha! Again, the other side of the scam is how good, legitimate organizations are dragged down! Before reading further, look back at the previous page and review the quality of the text on the click bait. It is fuzzy, not crisp. The text has been, for all intents and purposes, copied and pasted.

Suppose you or someone close to you – family or friend – replies to one of these emails. The person taking the call will sound very professional. They will “take your information” and connect you to their “fraud investigation unit.” The first thing required of you is to download software so they can help you. STOP! STOP! STOP! Disconnect the call immediately! No legitimate organization needs to access your computer!

These scams net over $60 million a year!

Please search for two of the scammer catchers on YouTube. One is “Scammer Payback” a.k.a. “Pierogi.” You can also type this link into your browser to watch a scammer get shut down, https://youtu.be/6xN_6joxx5U . The host uses voice changers to convince the scammer that there is a real mark on the phone. What the scammer does not know is that Pierogi is an IT expert and uses the access software to gain access to the scammer’s computer! Within minutes, Pierogi has deleted all the scammers files, including System32, which renders the machine useless forever!

The fellow who helped train Pierogi is a fellow named Jim Browning. He is so great at what he does, he can get into the scammer call center’s closed circuit television. You can go to https://youtu.be/le71yVPh4uk .

Often, scammers will want to have their victims buy gift cards, though some will send their victim to the bank to withdraw cash. The victim is told to mail the cards (or cash) to an address that is legitimate, but the addressee is fake. The package will be delivered by either UPS or FedEx. Scammers use them because they know, one, US Postal Service (USPS) carriers know their customers’ names. Two, using the USPS turns the scam into a federal offense initiating investigation by the U.S. Postal Inspection Service, the FBI, and Interpol!

The package will be met at the address by a “mule.” The mule’s job is to collect the package before the homeowner gets it. The mule will open the package, take at least one of the gift cards as a fee, and send the rest on to India. India is home to many of these scammer call centers. Most are embedded in buildings filled with other tech companies. Those scams netting $60 million above may have just 20 scammers. If the splits are even per person, that is $3 million *per scammer*!

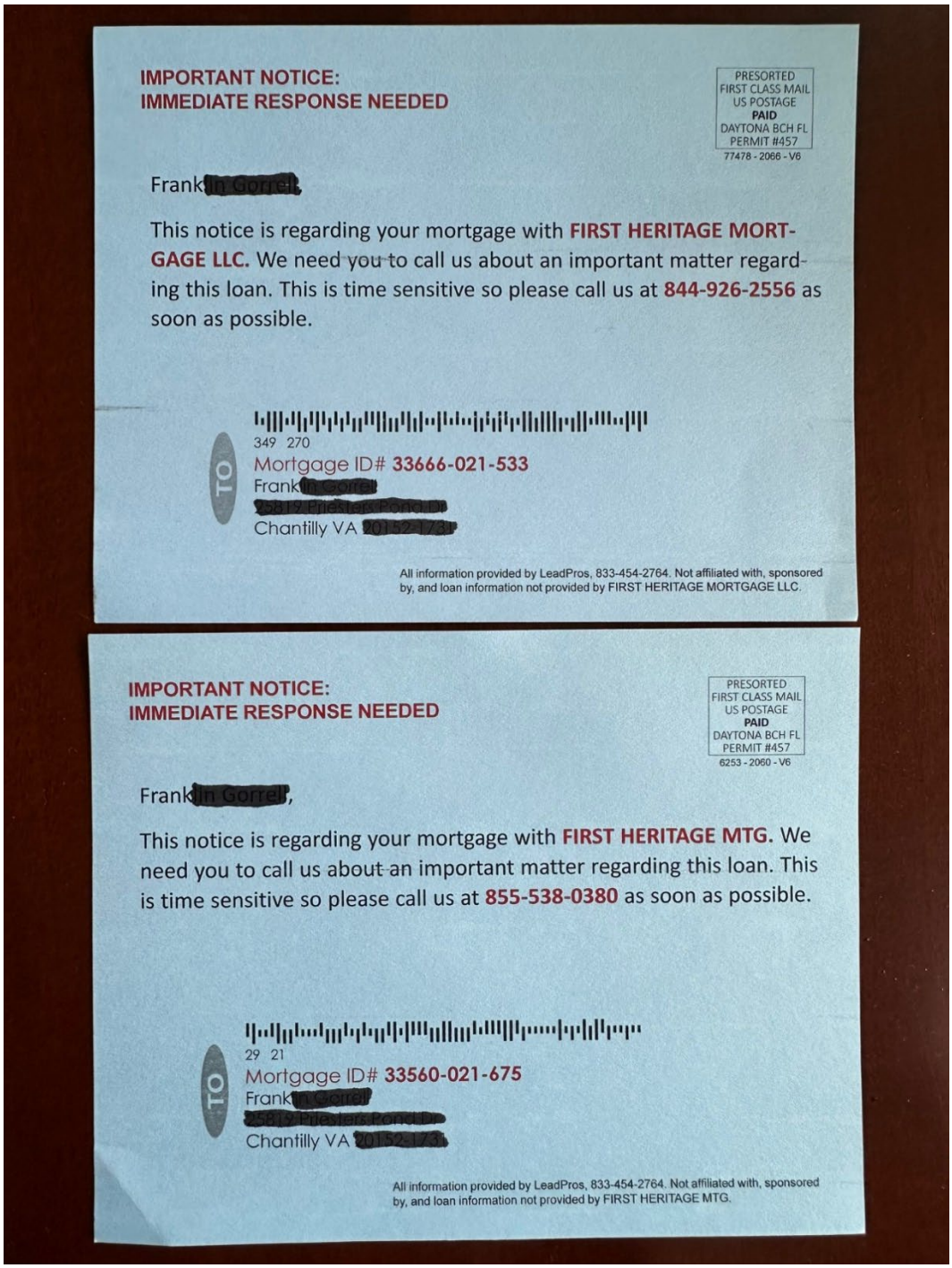
B. The new kid

No doubt by now you have been working with clients on getting the Beneficial Ownership Information (BOI) of their corporations, limited liability partnerships, limited liability companies, and other entities submitted to the Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN). This requirement imposed by the Corporate Transparency Act, which was embedded in the National Defense Authorization Act passed on New Year’s Day in 2021, has scammers circling like sharks at this golden opportunity! You may be aware that the fine for not filing on time is $500 a day! Scammers are already

trying to get this money. FinCEN reports fraudulent messages are being received by expected filers with subjects such as “Important Compliance Notice.” These emails include a link with a URL code or QR code. FinCEN **does not send unsolicited requests**! Alert your staff, clients, and anyone else who may (or will) receive one of these requests. They are fraudulent![11]

C. Double Bonus

There is no doubting the temerity of scammers. Look at the picture:



IMPORTANT NOTICE:
IMMEDIATE RESPONSE NEEDED

PRESORTED
FIRST CLASS MAIL
US POSTAGE
PAID
DAYTONA BCH FL
PERMIT #457
77478 - 2066 - V6

Frank[redacted],

This notice is regarding your mortgage with **FIRST HERITAGE MORTGAGE LLC.** We need you to call us about an important matter regarding this loan. This is time sensitive so please call us at **844-926-2556** as soon as possible.

TO
349 270
Mortgage ID# **33666-021-533**
Frank[redacted]
[redacted]
Chantilly VA [redacted]

All information provided by LeadPros, 833-454-2764. Not affiliated with, sponsored by, and loan information not provided by FIRST HERITAGE MORTGAGE LLC.

IMPORTANT NOTICE:
IMMEDIATE RESPONSE NEEDED

PRESORTED
FIRST CLASS MAIL
US POSTAGE
PAID
DAYTONA BCH FL
PERMIT #457
6253 - 2060 - V6

Frank[redacted],

This notice is regarding your mortgage with **FIRST HERITAGE MTG.** We need you to call us about an important matter regarding this loan. This is time sensitive so please call us at **855-538-0380** as soon as possible.

TO
29 21
Mortgage ID# **33560-021-675**
Frank[redacted]
[redacted]
Chantilly VA [redacted]

All information provided by LeadPros, 833-454-2764. Not affiliated with, sponsored by, and loan information not provided by FIRST HERITAGE MTG.

[11] Daugherty, Greg (4 January 2024). Corporate Transparency Act (CTA): Purpose, Implementation, and Recent Changes. Retrieved from www.investopedia.com/corporate-transparency-act-8413903 on February 1, 2024.

These postcards arrived just days apart. Of course, your author knew in an instant that it was a scam. Can you determine what may have tipped me off?

It was the mortgage company. It refers to the company that issued the mortgage—not the present mortgage holder! When the second postcard arrived, I noticed some significant differences. The holder's name, the bar codes (and associated numbers), the mortgage identification, the telephone numbers, and the numbers under the postage mark all changed. At least they had to keep the permit number. Of course, this puts the United States' oldest federal law enforcement agency on the case: the United States Postal Inspection Service.

IX. Conclusion

We covered the fraud schemes (long-term intent) and scams (short-term or one-time strikes). As for the latter we have no "internal controls" to prevent them. Common sense and a high level of skepticism is all that is required. Be certain to stay informed on these scams and warn friends and family – especially those age 60 and up – not to take the bait. In the next chapter, we look at internal controls to prevent and detect fraud schemes.

Controls to Detect or Prevent Fraud

Controls to Detect or Prevent Fraud

Learning objectives

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

- Understand that groups of fraud schemes have certain key controls to prevent and detect fraud;
- Understand that many of these controls can serve a valuable purpose in more than one group of schemes; and
- Realize that fraud is not always about money, but that our data is an asset that fraudsters will target.

I. Introduction

Internal controls over financial reporting (ICFR) are not new and we will not treat this chapter as if we are trying to unravel the mysteries of the Sarbanes-Oxley Act of 2002. Do you remember those conferences and seminars? There were hundreds of us CPAs gathered to hear how some company had "over 10,000 controls!" We questioned their sanity. Then we realized that was a bit of an overstatement. In many cases, it meant that there were IFCR controls, but there were also other internal controls over production and quality control. Often, what it meant was that the company had some 2,500 controls, with key controls tested four times a year, only 100 to 150 *key controls* were tested yielding 400 to 600 "tests." The total number of controls were added after multiplying by four. Realistically, it turns out that 400 to 600 individual ICFR controls are usually enough. However, we may find that there is some expansion in environmental, social, and governance with diversity, equity, and inclusion reporting.

Recall that in the prerequisite course(s), we focused on the 18 controls that were present at fraud victim organizations. We may touch upon a couple of those and add a new spin here but will not spend a great deal of discussion since we did that in the prerequisite course(s). We will look at some transactional level controls, calling upon various sources and ideas.

II. Prevent and detect asset misappropriation

This area has the largest number of schemes in several categories. It is the most likely area a fraudster will attack. Once again, we will use the i-Sight article as an initial guide.

Discussion questions:

When was the last time your organization reviewed all the internal controls in place at your organization?

How has your business model changed because of the SARS-CoV-2/Covid-19 pandemic? If you are working remotely, especially regularly, have you performed a review of the controls to assess whether modifications are required with remote work?

(Consider Surgent's 4-hour course *Internal Controls, COSO, and Covid-19* (ICC4), which reviews these issues.)

Let us look at some suggested controls beginning on the next page.

A. Background checks

You may recall from the prerequisite course(s) that this is a challenging control to institute. A criminal background check may indicate no problems. Other background check points may be impossible to obtain because people do not want to be sued for providing a bad reference costing someone an opportunity to get a position. A credit check may indicate bad credit, but that does not necessarily mean the person is more inclined to commit a fraud scheme. A devastating illness can harm credit.

And lest we forget, over 80 percent of all fraudsters caught are *never criminally charged*! In some cases, the evidence is thin. In most cases, the victim organization does not want to publicize what happened. We just covered how scammers rely on embarrassment to prevent victims from coming forward.

The best course of action is to do as much as possible. Social media is free and can tell a lot about someone.

The best hint that something may be wrong will come with an in-person interview. More than one is suggested, though a panel of interviewers can provide feedback. Choose a panel or team with different backgrounds but who understand what the job's requirements entail. Each person takes note during the interview. After the interview is completed, the panel or team will discuss impressions, though it may not be right away. Do some research on methodology and find what feels right for you and your organization.

B. Implement checks and balances

This is a fundamental element of ICFR and all other control areas. No single transaction should pass through the system, accounting or otherwise, without at least two sets of eyes reviewing it. This is a basic concept. No single department can procure goods or services without concurrence from another, related department.

For example, if someone wants to obtain a laptop, the person, their supervisor, and the head of IT, or designee(s), must sign-off on the purchase *before* the purchase request will be processed by Purchasing into purchase requisition.

When received, the laptop must be officially received, and any other internal procedures followed. These might be relative to getting the laptop ready for use by the requestor. It will include logging by the IT Department and be assigned an asset number and will be tracked and checked for its presence periodically, at times unannounced, to ensure it is where it is supposed to be.

The receiving report, purchase request, and invoice will be matched before invoice payment.

C. Separate functions of preparer and signer[1]

This ought to be second nature by now. The person who prepares a check, ACH/EFT payment list, a request for purchase, and so forth is different from the person who approves it. In addition, there is another person who executes the transaction(s), if possible. This is not about questioning someone's integrity (although it certainly seems that way). Consider that what this "segregation of duties" really does

[1] We are following the i-sight.com article *41 Types of Fraud and How to Detect and Prevent Them*, and in this article this control is "limited" to checks. We believe that this control has benefits in several places, as explained above in discussing checks and balances.

is ensure that someone cannot be falsely accused of theft. Everyone in the organization feels more comfortable.

Let us take this up to management and the C-suite. Certain transactions, especially the “financial statement” transactions, require at least one senior manager to concur.

D. Rotate duties of employees in accounts

This refers to accounts receivable and payable, but also includes when certain entries go into the general ledger. These include depreciation and amortization. It also includes those entries related to allowance accounts and the equity section.

Just like no one person should handle both cash receipts and disbursements, and neither should “balance the checkbook”, someone ought never be in accounts receivable or payable for a long time. Similarly, the person handling other general ledger adjustment should not be in that role for years and years. The possibility of fraud increases each year.

Recall the **accounts receivable fraud schemes**: Lapping, skimming, fake write-offs, fictitious sales and/or accounts.

Consider this advice from i-Sight.com:

> Is your employee constantly debiting the wrong accounts? Are they “accidentally” misplacing or tossing statements, or billing customers at weird intervals?
>
> There are a few things that might be at play: either your employee is really [unbelievably] bad at their job, or there’s fraud taking place in your company…
>
> Sometimes you might get lucky, and an employee unintentionally learns about the fraud, other times an audit exposes the truth, or someone reports their suspicions.[2]

There are specific red flags when fraud is afoot in accounts receivable. Referring to historical data, assess whether there is an excessive number of discounts, write-offs, voids, returns, or other modifications to accounts. These oddities may signal skimming of payments. Be certain to assess both the number of instances and the dollar amounts involved.

If customers report unauthorized sales or you notice suspicious customer accounts, this may flag an employee is creating fictitious sales and/or accounts. Sending customers’ statements or providing a portal for them to view their account information, including recent transactions and account balance is a quick way to take the shine off these schemes.

This portal can also alert your customers or clients to sudden account activity or other discrepancies. Your frequent review of data can also stop a scheme. Is there activity in an account that has been historically low in activity, or is considered “dead”? Is there a sharp increase in sales, revenue, or accounts receivable balances?

---

[2] Ibid.

Perhaps the one “control” that we do not think to incorporate is listening to our customers or clients. Are they complaining about receiving a non-payment notice when they mailed the check in September, but the payment was not recorded until November? (Lapping?) With a portal for them to view their activity, they may tell you that a sale is bogus. In fact, lapping is a very tiring scheme to pull off because the fraudster must wait for funds to appear to pay the aging receivable.

Let us turn our attention to **accounts payable fraud schemes**: shell company, billing fraud, check fraud, vendor master file fraud, and invoicing fraud (kickbacks). Fraud may be detected several ways according to i-Sight.com:

- Conduct regular internal audits (every few months) as well as surprise audits. (This internal control is rarely used but can both prevent and detect schemes early!)
- Implement a hotline where employees [and vendors] can report concerns or incidents of internal fraud (ethics or fraud prevention hotline).
- Set up surveillance measures such as security cameras.
- Have an employee who doesn’t work in AP manually review your financial records (related to AP and cash receipts).
- Use automation to detect anomalies in your records (such as Benford’s Law and other automated information system controls; and an automated notification of past-due payments from customers).
- Identify the owner of all PO boxes on vendor files.
- Compare employee names, initials, addresses and other contact information against vendor files.
- Manually validate vendors’ legitimacy via email, phone, or in-person contact with a representative.
- Review transactions’ red flags for fraud such as round numbers and unusual invoice frequencies or amounts for the vendor.
- Require all AP employees to take their allotted vacation time and designate another employee to take over their duties while they are away.[3]

Some of these suggestions may be controversial. Between AR and AP, performing these controls may be a full-time job, suitable for an internal audit or fraud prevention team.

This ties nicely to the suggestion of **conducting random audits of company accounts**. These would be accounts that your organization’s fraud risk assessment deemed susceptible to fraud.

E. Delay commission payment until goods/services delivered and confirmed

This does not mean that there could not be a return of unwanted goods within a window for returns. This ensures that a commission will not be paid on a fake sale. For a fake sale to yield fake commission payment, there must be at least two people working the inside – one on each end. This means there are two sets of internal controls and more sets of eyes watching for phony sales and purchases.

F. Keep checks in a locked cabinet and destroy voided checks

With the use of checks fading fast, this control may be getting close to passe. However, if checks are needed from time to time, for whatever reason, make sure they are locked up.

---

[3] Ibid.

Also be alert that returned checks should *not* be voided and destroyed immediately. Check the jurisdiction in which you operated and that of the addressee to ensure compliance with abandoned property laws.

G. Conduct due diligence when setting up vendors

You want to verify the vendor's business name(s) by checking the Secretary of States Corporate Registrations for the state in which the vendor is formed (Delaware being popular). Also confirm the taxpayer identification number (TIN), the street address and, if relevant, the PO Box, bank account (for ACH/EFT), and vendor contact.

When checking the corporate documents, check for employee names.

H. Use data mining to uncover anomalies and patterns

This control and process may reveal issues with vendors, customers, and "employees." You can use this to compare vendor addresses with employee addresses.

You can review master vendor file management to check for change dates and information that changed. You may also check vendor master file to ensure billing volume is reasonable and consistent with prior periods, even taking into consideration seasonable ebbs and flows.

Discussion questions:

If your organization is no longer using checks, has the organization implemented controls over ACH/EFT?

Do your vendor setup procedures include any due diligence to ensure the vendor exists?

Are there any other opportunities to use data mining?

III. Accounting fraud

The schemes in this category include embezzlement (larceny), fake supplier, personal purchases with organizational funds, double-check payment, and accounts receivable.

Several controls discussed above assist in this area. Those include tight internal controls over accounting functions, segregation of duties (separate setup and approval functions), random audits, and rotation of duties. Additional controls follow.

A. Outside contractor performs review and reconciliation regularly

This means the organization hires a trusted firm to perform a review and reconciliation of the accounts, such as receivables and payables, sales, cash, and any other similar accounts the organization has. As hinted in the subtitle, these reviews occur at regular intervals. Your author experienced such reviews when working for a retail athletic shoe store. The company had an internal audit department that routinely visited stores in the chains. There were several brand names. The auditor would call to say when the auditor would be there so the manager would have staff to cover the sales floor so the manager could sit with the auditor if needed. Routine audits were not a problem. You may recall the story of "Mr. Burns" in the prerequisite course(s) about what happened when the auditor appeared for an unannounced audit; and this resulted, probably in conjunction with a hotline tip, in the manager's termination for cause.

B. Mandatory vacation time

This control was discussed in the prerequisite course. It is one of the 18 internal controls frequently present at victim organizations. It is an opportunity to unveil a scheme by someone who is filling in for the fraudster – assuming the fraudster does not "forget" to take mandatory time off. The best practice is five consecutive workdays.

An additional feature of this control must be to check each day the person is supposed to be on vacation if the person logged into the system. With remote work becoming more popular, people could log in from anywhere! This could be to cover their tracks, or pull off the fraud when people think they are not logging in. Information technology controls ought to cover this.[4]

C. Automated positive pay

According to Investopedia, "Positive pay is an automated cash-management service employed by financial institutions to detect fraud. Banks use positive pay to match the checks the company issues with those it presents for payment. Any check considered suspect is sent back to the issuer for examination."[5] Simply stated, the organization's bank issues a check for $50.00. The check is "presented" for $500.00 at the organization's bank. It appears it has been altered. The bank alerts the organization.

The group of controls are focused on stopping **payroll fraud**. Those schemes are ghost employees, advance fraud, timesheet fraud, and paycheck theft. There are two controls we have discussed above that help in this area: mandatory vacations and separating the tasks of preparing payroll checks and reconciliation of payroll accounts (segregation of duties).

D. Reconciliation of balance sheet and payroll accounts each quarter

This is a handy control because payroll tax returns are due each quarter, Form 940 and 941. This could be "contracted" out as discussed above at 3. A. The organization's controller and chief financial officer ought to have a rough idea of what each payroll is going to total. And since these persons ought to be watching the financial data, they will have an idea of what a quarterly total should be, give or take some amount. This control ought to be able to spot odd entries on one side or the other. Consider payroll disbursements that do not have withholdings.

E. Require managers or supervisors to approve timesheets and overtime claims

There may be times when overtime is necessary. As CPAs we certainly have times during the year when overtime is expected. Your organization may have this need, too.

Placing the burden of approval on managers and/or supervisors adds to their need to ensure that hours are recorded properly. Suppose a manager approves a timesheet for someone that includes overtime, which is paid one and a half times the regular hourly rate. However, another employee is suspicious of the overtime, and calls the organization's ethics hotline. The Ethics Officer pulls badge swipes for the employee and confirms that the employee badged in around 8 AM each morning and badged out no later than 4:30 PM each afternoon. With a half hour taken for lunch, the overtime claimed seems excessive. How might the manager feel when the Ethics Officer presents the information if overtime claimed for the week exceeds 2 ½ hours (which would be working through lunch)?

---

4 Ibid. *41 Types of Fraud…*

5 Kagan, Julia; Anderson, Somer (Reviewer); Beer, Katherine (Fact Checker). (2021, August 15). *Positive Pay: What It Is, How It Works, vs. Reverse Positive Pay.* Retrieved from www.investopedia.com on January 20, 2023.

F. Restrict ability to modify pay rates and hours

Payroll department employees may have access to make such changes, but any change would require concurrence from the payroll department manager and at least one of the Accounting Manager, Controller, and/or Chief Financial Officer. Embedded in the electronic data must be a reference to the requesting item. For example, it may be a payrate increase carried over from the Human Resources system. It may be a timesheet correction submitted after the timesheets were processed. In many organizations, this happens depending on when timesheets are due. If due before the actual end of the week date, corrections may be frequent to correct the one or two days estimated.

G. Perform data analytics

In the i-Sight article we are using as our basis, the actual control suggested is, "Perform data analytics on payroll records to look for matching addresses, names, bank accounts, etc." Yes, this is a good start. Your author recommends looking for matching Social Security Numbers. Tailor the analysis to search for names and addresses that are close – think an intentional misspelling or added/removed middle initial.

Your author also encourages you to go one step further. Run a pivot table looking for mismatched data from the Human Resources' database. Doing this may show that a bonus was paid that did not pass through HR for approvals. It may also show someone getting a higher payrate in the payroll system than the HR system has approved. The analysis may also yield another fault, that is the next control that can be performed separately and pays off better when performed on a regular basis.

H. Ensure terminated employees are removed from the payroll

This is a situation where an employee gives notice, let us say on the first day of the month. The last day of employment will be on the fourteenth day of the month. Given the payroll cycle, the final pay will not be transmitted via ACH/EFT until the twenty-seventh day of the month. This control depends on the payroll system that the organization uses. It is possible that the software will permit a termination day and last pay period paid date (which might even automatically be filled in).

When off boarding the employee, personnel in HR ought to include in the checklist, reviewing when payroll payments to the employee will end. Consider consulting with your organization's legal counsel as to wording options and whether to include a warning that if an "extra" payroll deposit is made after a certain date, the off-boarding employee may be subject to legal action.[6]

IV. Corruption

Our guiding article refers to this area as "Bribery and Corruption." The former is generally limited to cash or some other item or favor of value. These seem as though they are closely linked to one another. We mentioned the movie The Sting in an earlier chapter. Early in the movie there is a scene that discusses the corruption of the Chicago area police and politicians. Later in the movie, Paul Newman's character explains how grifting was run like a business saying in part, "The fix was in. The [police] took their cut…" And this is one reason scammer call centers abound in parts of India – corrupt leaders in politics and policing. The bribes are a cost of doing business. Thanks to Browning and Pierogi, though, the pressure and embarrassment is building. Meanwhile, here are some controls that can be instituted to reduce the chances of corruption however it may be manifested.

---

[6] Ibid. *41 Types of Fraud…*

A. Strong code of ethics

A code of ethics and business conduct is only as good as the paper on which it is written – if it is on paper at all. The full suggestion here is, "Have a strong code of ethics and ensure everyone in the company, from the top down, knows what it says and puts it into practice."[7] This is the first of three interrelated controls. Ethics training is important. Reminding people what the code of ethics states and what it means is vital because it may get someone's attention at just the right time before they stray. It may also prompt someone to call the ethics hotline.

In order for the goal as stated in this control to be met, regular training in the code of conduct and ethics will have to take place. Training once a year may not be enough to achieve the goal. Monthly may be too much time to spend away from regular duties. Perhaps once a quarter will suffice. Find what works best for your organization's personnel. The best way to do it is to include not just staff level, but senior staff and executives to have a discussion. Imagine the CFO or CEO making a statement about what this particular section of the code means to them! Impactful! This ties nicely to the next control.

B. Top levels set examples

As completely expressed in the i-Sight article, "Ensure those at the top levels of the company set an example that makes it clear that bribery and corruption are not tolerated." The limitation here may be that the vast majority of people who are approached for a bribe or to behave in a corrupt manner are not going to say, "No!" and then say anything that could hurt the person making the pitch. Consider a vendor's company is struggling financially and calls a senior contact at your organization, say the CFO. The vendor offers a kickback, that is a bribe in a different form, for the CFO to approve a certain purchase. The CFO politely declines.

That is good. However, what should the CFO do now? If the CFO calls the other company's ethics hotline, that employee could suffer devastating consequences. Conversely, the CFO could assume that the vendor employee is having a hard time, and in a few days, may be better. Perhaps a follow up call to check on the vendor employee's well-being will suffice.

No matter how the CFO handles the situation – and this is a good one to discuss with your team – can the CFO share the experience with the CFO's personnel? The CFO could say to the personnel gathered, "Not too long ago, I had an experience with a vendor…" That addresses this control.

Discussion question:

Do you have sessions such as these, or an experience or two that you could share to help reinforce the importance of ethical behavior?

C. Discipline employees who breach the company's code of ethics

This means that the example set by organizational leadership is not just for looks. The critical issue here is consistency. An organization will lose credibility very quickly if consequences for violating the ethics policy are not consistent. In fact, it is a good idea to include the types of consequences that *will be enforced* within the code of conduct and ethics. For example, if someone wears inappropriate attire to the office, the person will be told not to wear that outfit or item again. If there is something offensive (such as

[7] Ibid. *41 Types of Fraud…*

a tee shirt with words and/or graphics), the person will be told to either turn it inside out or go get an appropriate top.

If someone is late to work, it is mentioned the first time. It is mentioned and noted in writing the next time. It goes to HR for additional disciplinary action the third time. This means termination is possible.

Should someone be caught stealing, in any way, the discipline is… . The organization continues to explain the various disciplinary steps for each group of possible offenses. In addition, possible consequences can be mentioned for other breaches of the code of ethics that are not specifically mentioned, but that do fit into one of the categories in the written policy.

This control works best when it is in writing and emphasized in the on-going training and re-training.

D. Conduct due diligence on third parties with whom you do business

This goes beyond speaking to references the potential business partner provides. Certainly, if you want to bring in a cleaning service, the company will give you names of contacts who will provide a good reference. You must search online for bad reviews. Keep in mind that some bad reviews may be from sour grapes. For instance, the review appears to be from a “former customer”, but is from someone who was fired by the company. Contact the Better Business Bureau in your area. Look for postings on social media.

You must also check the Secretary of State’s website for corporations to assess if there is any potential conflict of interest, and if the company is in good standing.

You may even visit the company’s website and physical location.

Interview the contact person in-person. Do you believe they are being truthful? Do they give you the willies? Do they maintain eye contact or avoid looking at you? Do they ask for a cup of water? If so, their dry throat may be due to not being truthful with you.

Keep one important thing in mind: the third party company’s point of contact and leadership may be completely honest, but the ACFE reports that this third party company has at least one fraud scheme in their organization, too. You want to avoid inviting a fraud scheme into your organization.

The next control involves you doing “double duty.” That is, a control you put in place for your organization that will also benefit your third party business partner.

E. Look for product substitution red flags

This control suggestion from the i-Sight article is good. What are the possible red flags?

The first red flag is if you acquire parts or equipment that require a *high number of tests or have high number of failures*. For instance, if you bring in a laptop and it takes longer to set up than what would be expected, maybe someone has to go deeper to see if the laptop is what it appears to be. If you acquire parts, and they fail at a rate higher than expected (read also, as indicated in sales materials), then it may be a knockoff part.

The second red flag is closely related to the first: *unusually high numbers of repairs or replacements*. Suppose you are a heating, ventilation, and air conditioning (HVAC) installation and service provider. You discover that you are receiving an inordinately high number of calls to service air conditioning units. Your repair teams come back with the same issue, no matter which call, the coil was leaking freon. Until gathering this data, you believed that the freon replacement would be enough, but with this new information, you begin to wonder if the manufacturer knows that the coils may be bad. That is just part one.

What if you also were the company that installed all these units? You check the records to see which of your technicians installed the units, hoping to find several names. If you find just one name, the common link to all these flawed units, you may have a serious problem. Could it be that the coils were replaced with a lower quality coil and the original coils sold for their copper value?

You go to your warehouse where these units are stored. You observe that the boxes have been resealed, and you notice that a third red flag of production substitution is visible on several of the units. There is a *lack of warranty information in the packaging*. In fact, the plastic sealed envelope on the side of the boxes has been torn off. If you ever open a box that does not have warranty information inside, contact the seller immediately!

The fourth red flag is that the item is in *unbranded packaging*. No company wants to deliver its products in packaging that does not also advertise its products. It is basic marketing. It makes no difference whether it is a new phone, a case of wine, a computer; logos and other trademarks will be on the packaging. Even when the packaging is placed out for the recycling truck to pick up, it is advertising the product.

One caveat here, though. You may wish to cut the box up into smaller pieces that can go into a curbside recycle bin rather than let unscrupulous people know there is a new flat screen in the house. In fact, you can dispose of the box over several pickup cycles.

The fifth and final red flag is when *products do not look like the products ordered.* This is one that is more likely to occur with an online purchase. We discussed the scam where the target receives an email saying that their purchase has been approved and here is a phone number if you have any questions. This variation is a cheap knockoff, which may not even work at all and has to be returned, but “you will have to pay the shipping fee that will be refunded to you when we receive the [insert item here].” However, it could be a fraud scheme.

Consider two people who are involved in the scheme. One works for the shipping organization. This person replaces the requested and required item with the fraudulent substitution. The other person in the receiving organization signs for the product as if it were the proper item. Questions may still be raised. It is important that you make sure that folks requesting items are part of the process to accept delivery. On the shipping side, those who take the orders should be able to ensure that the proper items are shipping. Having an additional set of eyes on both ends helps.[8]

That ties in nicely once more to the next control, one we did discuss in the prerequisite course(s).

---

[8] Ibid. *41 Types of Fraud…*

F. Conduct risk assessments for weak points

What are the areas you need to watch more closely? This is the question you want to answer with the risk assessment. We are focused on preventing and detecting bribery and corruption, but this risk assessment ought to be conducted for the entire internal control system. What weaknesses may exist that would permit bribery and corruption to take place?

Check your organization's morale. Good morale will mitigate risk while poor morale will increase risk. This is why walking the floor and listening to people is so important. You can also use anonymous surveys to assess morale. Are people engaged in their work? Are they satisfied with the workplace? DO they feel valued? This last question is key because it goes beyond the paycheck. An organization could pay someone twice as much, but if the person feels like no one is listening to them, or cares to hear an opinion, the money is meaningless.

Review processes to determine if there are places where there are no back-up controls. Are there any places where a control is performed, but the control is not confirmed complete by a second party? Are there any controls that are difficult to prove they were performed? For example, in the product substitution scheme above, it appears that no one on either side of the transaction double checked the product shipped and received against the order documentation. If there had been, the "wrong" item never would have been shipped.

Your organization has several places where you can assess risk, and you know it best. If you are in public practice, this is a great opportunity for you to add value for your clients. Have the conversation in their offices. It is not that you suspect someone. It is that you want to help your clients have a successful business. It also gives you an opportunity to assess the morale at your clients' business. You could prevent losses.

G. Train all employees on bribery and corruption prevention

Consider that a fraud scheme may start with a scam. Or consider how someone becomes addicted to a substance. The person does not down twelve beers the first time they sneak a drink. A person does not turn to heroin without trying marijuana first. Well, an employee may be corrupted with a simple scam by someone inside or outside the organization. This is why it is vital that all personnel are alert to what could be an invitation to get into deep trouble.

Let us return to the product replacement scheme above. How did it start? One person said something to the other person. This means that one person *corrupted* the other. You want your personnel to know that anyone offering money or other gifts in exchange for "looking the other way" or "going along with it" (whatever the "it" is), is wrong and must be reported to leadership or the Ethics Officer immediately. You see, it starts innocently enough. "I need a quick favor, it won't hurt, and I'll give you a hundred bucks for your troubles." That is how the hook is baited. The explanation makes the act seem harmless enough. Who is really harmed? And there is a hundred dollars in my pocket.

It is that payment that the primary schemer uses to expand the fraud. "Hey, you know I could always tell someone you took a hundred bucks to (fill in the deed here)." With that, the hook is well into the other party's cheek, and they are reeled in by the primary schemer. It happens a lot.

Make sure everyone knows what is and is not proper business conduct and what is expected of your staff and business partners.

H. Reward ethical behavior

Many years ago, your author brought home a Dachshund puppy. His name was Fred. When your author told people that Fred was house trained in 24 hours, people could not believe it. How? I caught him doing it right. First, before taking him out, I showed him how to scratch at the door. Then I opened the door and went out with him. When he went "to the bathroom" outside, I praised him with a happy voice, and lots of affection. In just a few hours, Fred went to the door on his own. You see, people and puppies have something in common. We want to be rewarded for doing things right!

It is true. Rewarding ethical behavior will go much further than disciplining those who violate the code of ethics. There are those who might say that rewarding someone for doing their job is what a paycheck is for. A five hundred- or thousand-dollar bonus for reporting an attempted bribe will get everyone's attention. Showing appreciation will build long-term loyalty, too. That could be priceless.

V. Data theft

This is the Lost City of Gold, the Templar Treasure, and the Holy Grail for grifters. Chances are not only your personal data is on the Dark Web, but company data could be there, too. Your organization's servers are a tempting target – both outside and within your organization. Let us review what can be done to make the pilfering problematic.

A. Restrict access to proprietary information

There is no reason for the controller to have detailed information about employees. Limit access to the information necessary for the performance of a person's duties. In fact, employees should not know what information they cannot see. The restrictions are embedded in the information system.

This also means that the information ought to be hard to find for anyone searching for it, again, whether within the organization or outside the organization. Folks in accounts receivable do not see information related to accounts payable. Payroll personnel can see pay and bonus information, but do not see any other personnel records. Human resources sees more than most, but may not see the accounting and finance folders, nor anything related to audits.

The best way to restrict access to proprietary information is to hide folders from those who do not need to see them. They do not know they exist. If they were to click on a folder and a message popped up stating, "You do not have permission to view this folder", then the game is on. People have more advanced information technology skills now. You need to have trustworthy personnel watching and preventing unauthorized access.

B. Set up IT controls to alert for certain activities

Management is alerted whenever a large data download occurs. Some of these may be legitimate and expected – such as at monthly, quarterly, and annual closing. The alert confirms the successful event. If downloads or transfers occur at an odd, unexpected time, this may be a problem.

Before any new download or transfer that has been requested may occur, consult with the IT department. Even if it seems reasonable, it may be harmful. Who is making the request? Why is it needed? Downloads and transfers happen for audits. The auditors have a complete copy of the general ledger and can perform the auditing procedures with ease. It is great, especially if they can do it all in their office rather than take up space at your office. But it is important that your IT people talk to their IT people about

how the transfer is to take place and where the data will be stored. Moreover, how is it protected behind their firewalls?

C. Software that alerts management of suspicious network activity

Purchase software that provides alerts to management and IT when an employee is trying to access sensitive information outside their job duties' needs. Keep in mind that it may not actually be the employee! It could be a hacker who wormed their way into the system.

D. Dispose of confidential information properly

When paper documents are no longer needed, especially if electronic versions exist, the paper ought to be shredded thoroughly. Have your IT department remove electronic data from electronic devices before the electronic devices are redeployed or destroyed. If the data is no longer needed on the network, but may be needed in case of audit or legal matters, ensure the data is stored where the proper person(s) may retrieve it – possibly on a standalone system.

E. Use strong passwords to access sensitive data

By now we all know what makes for a strong password. Not only should the password be strong, but it ought also to be changed at least every six months.

In addition to strong passwords, at least once a year, the access profiles of all personnel ought to be reviewed to ensure that accesses that are no longer needed have been removed.

If personnel do rotate responsibilities as discussed above, changing accesses could be a full-time job for someone in the IT department.

F. Clean desk policy

This policy prohibits personnel from keeping sensitive information on their desks for any and all to see when they are not at their desk. In fact, it includes a "clean desktop computer." This means that the employee must lock their workstation any time they walk away from their desk. Inputting the password again only takes a few seconds. The harm that could be done from an unlocked workstation by a bad actor in just a minute far outweighs the "inconvenience" of reentering a strong password.[9]

Since login identities and passwords have to be stored somewhere in the system to verify the person logging in, go a step further and require a fob with changing codes, such as SecureID™. It would have to be an amazing guess!

VI. Conclusion

We have reviewed some general controls, and there is no doubt that you have these and more in place. Be sure to test the controls, even if your organization is not subject to the SOX requirement. Take nothing and no one for granted. Let your personnel know how much you appreciate them. This alone will do more to boost morale than you may realize. And think of other ways you can show appreciation. Surprise the team with a buffet lunch or consider providing bonuses in the form of travel rather than cash (though cash is good, the memories from a great trip are priceless). Noncash bonuses for a group, team, department, or division might also go a long way toward instilling good will from the employees.

---

[9] Ibid. *41 Types of Fraud…*

In the next chapter, we will look at some checklist and assessment tools you can use to assess your organization's fraud prevention health.

Checklists and Assessments

Checklists and Assessments

Learning objectives

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

- Comprehend that there are tools we can use to assess and improve our systems;
- Understand that checklists are one such tool but that they cannot perform processes and procedures; and
- Realize that there are different approaches to utilize to achieve our goal of an improved control environment and fraud deterrence.

I. Introduction

We have reviewed various fraud schemes and broad descriptions of the controls that help us prevent and detect those schemes. Before we look at tools that can be used to aid in assessing our overall control system, it may help to look at a tool that can aid in our processes. It is the flowchart. The advantage to flowcharting our processes is that we can see if we have steps in the proper order. We can also ensure that we include all internal controls – not just those for financial reporting – but others as well.

For instance, our Cash Receipts and Disbursements flowchart will cross reference to Accounts Receivable, Accounts Payable, Payroll, and other asset and liability accounts. Human Resources process flowcharts will cover on- and off-boarding, which will have connection to Payroll.

If you have ten controls for a certain area but can only find a reference in your flowchart(s) for eight or nine, then you are missing something. Of course, if you have ten controls and all ten are covered, some more than once, that may be an indication of a strong internal control environment.

II. Checklist example

You may want to search the Internet for various checklists, but it may be best to either discuss with your accountant or with your clients, depending on which side you find yourself. Checklists are a very helpful tool. If you watch the movie *Apollo 13*, you will see the astronauts use checklists (alternately referred to as a procedure). Pilots use several checklists in their work. There is a checklist to walk around the aircraft and check wings, fuel tanks, lights, ailerons, elevators, and rudder. There is a checklist to turn over the engine (or engines). There is a checklist before they taxi, and before they tell the tower they are ready to taxi and before they tell the tower they are ready for departure. There are checklists after takeoff, and at other times in flight. Of course, there is a checklist preparing to land, right after landing, and preparing to shut down at the gate. It is not that pilots cannot remember all that – after a while, no doubt they do. The checklist is a prompt to ensure that they do not forget anything!

We all have the experience of heading out to work, only to realize that we forgot something. Maybe it was lunch, or the cell phone, or something needed for a meeting. No matter, we all forget from time to time. Do you walk around your vehicle before getting in to start the engine (or motor)? Do you check that your windshield wipers and turn signals work? What about the brake lights? Probably not. If you think cars are smarter now, you should see aircraft. They literally can fly themselves. In fact, in an emergency, they can land by themselves, too!

A checklist is a powerful tool, but it will not prevent fraud – just like the checklist in a cockpit cannot start the engines.

Discussion question:

> Before moving on, do you and your organization utilize checklists for certain tasks, such as when on-boarding or off-boarding personnel? Is there a checklist relating to certain expenditures and whether the organization ought to incur the costs?
>
> Could you think of a way to utilize one or more checklists to improve compliance, internal control function, or other business processes?

One example your author found was cleverly titled "Fraud Prevention Checklist" from the University of California, San Francisco. It is four pages long with forty items. The choices to check or circle for each item are Y (Yes), N (No), DK (Do not know), or N/A (Not applicable). At the top of the first page is a very important purpose statement.

> This checklist is designed to assist departments [to] assess their current internal control strength and fraud risk. The checklist is divided into process categories and will act as a guideline to identify areas where departments can improve their controls and lessen the risk of fraud.[1]

Key words to note in that paragraph are:

- **[T]o assist**, meaning that those using the checklist ought not expect that forty *Yes* responses means that no fraudulent activity can occur or has occurred.
- **[C]urrent… internal control strength and fraud risk**, meaning that there is the possibility, even probability, that the system may weaken, and risk increase should anything change. For example, if the organization moves to a new software or some update, controls may not work the same. If there is turnover in the department, there may be a loss of institutional knowledge that could upend processes. No matter what, this is not intended to be a one-time exercise. It will be reperformed at least once a year.
- **[G]uideline**, meaning that one may think of additional areas to add to the list as policies and procedures evolve.
- **[I]mprove**, meaning there is an ongoing purpose to enhance the internal control system. In the instructions paragraph, the user is advised, "If you have a significant number of 'No' and 'Don't Know' responses, consider whether a more formal review is warranted."[2]

Four of the five sections are relevant to just about all organizations with modest adjustments. Those sections are:

1. IT Controls and Cyber Security (Items 1 through 5);
2. Cash Receipts and Accounts Receivable (Items 6 through 19);
3. Cash Disbursements and Accounts Payable (Items 20 through 30);
4. Awareness Training and Reporting on Fraud (Items 31 and 32); and
5. Sponsored Award Administration (Items 33 through 40).

We will not reproduce the entire checklist here; the link is just below. The following are a few items that are worth noting:

---

[1] Checklist retrieved from https://fraudprevention.ucsf.edu on September 28, 2022.
[2] Ibid. p. 1

(2) Do employees know how to identify and delete phishing emails or report to IT Service Desk if they have mistakenly clicked on a link?[3]

Even a "yes" answer here may not be enough. Ideally, when a phishing email recipient can clearly identify a possible, even probable phishing email, a method of forwarding it to a Cyber Security Team is a huge help. What if someone clicked on the link and had no idea there was malware lurking in the message? The methods a Cyber Security Team may employ are well beyond your humble author's abilities. However, they could prevent further attacks, or even reveal a vulnerability previously unknown by understanding what the malware was sent to target. Consider all the valuable data your organization has on servers.

(4) Does management perform periodic system access reviews to ensure employees only have access to systems they need to perform job duties and to ensure the level of access is appropriate for employee's responsibilities?

There are times when necessity leads to someone gaining what was supposed to be short-term access to some area in the systems. If job rotation is a control put in place, this review may occur on a more regular basis. If not, and folks fill in for others on vacation, then some access information may be left intact, albeit inadvertently.

(5) Does the department ensure all staff have taken the annual Cyber Security training?[4]

This may be something new to consider, especially after our review of item (2) above. The critical point for us is that the training ought to occur at least once a year. Scams and methods of attack change. It is important for personnel to be informed.

(10) For cash receipts received through the mail, do you have two individuals opening the mail and logging the cash receipts?

For many organizations today this may be a quaint reminder of days gone by. Yet, it still may be needed in some organizations. This is segregation of duties. Suppose Person A opens the mail and Person B logs ten checks received, recording payor, amount, check number, and anything in reference area. From there, the stack of checks goes to Person C for logging or preparing the deposit. The total for the receipt log and deposit log must match.

(19) Are vacations required for individuals handling cash, and cash disbursements so that someone else can temporarily perform their job function?[5]

This is designed to interrupt skimming/lapping. Consider the discussion above regarding item (10), if persons A and B are colluding, person C does not know money is missing. If person A is colluding with person C, person B is unaware of missing checks. Management review of cash receipts and deposits will help. Management also needs to know if a customer receives a past due notice they state is unwarranted and can prove the check cleared.

---

3 Ibid. p. 1
4 Ibid. p. 1
5 Ibid. p. 2

Discussion question:

Given the discussion of mandatory vacations in this course, if the control is not present in your internal control system, and given that several schemes may be detected (perhaps admitted) without enforcement of this mandatory control, do you believe implementing this control ought to happen in your organization?

If you cannot implement it on your own, do you know the key personnel to whom to pitch the idea, and are you already thinking about the pitch?

(21) Are invoices greater than $500 reviewed by someone other than the requestor?

(22) Are invoices greater than $5,000 approved by a secondary approver (someone who was not the original approver)?[6]

Your organization may have different thresholds. For item (21), your author would rephrase it this way, "…by someone in addition to the original requestor." The requestor ought to sign off that the product or services has been invoiced as received and as requested. The request was for one hundred widgets and we have been properly invoiced for one hundred widgets. The requestor ought to have been informed if fewer (more likely) or more (less likely) widgets were received. Therefore, the requestor ought to know what to expect on the invoice.

Item (22) makes clear that the same person cannot approve an invoice greater than $5,000 twice. Personnel in the accounts payable group will not be invoice approvers except for timesheets for any temporary help [more in line with what is described in item (21)], and the manager's approving timesheets for accounts payable staff. What risk exists with these two controls?

If "splitting" popped into your head, that is a good thing. Invoices, even the orders themselves, may be split to avoid thresholds. Review your vendors' websites for information on ordering that will reveal these thresholds. Call someone at the vendor if needed. Two orders of fifty widgets as presented above, allows the $500 threshold to be evaded. Yes, evaded. Just as in taxes, avoiding a tax by not buying something is one thing; evading the payment of a tax that is incurred is something else.

Approvers ought to make themselves aware of what they are being asked to approve. They need to consider that their approval may implicate them if there is a fraud scheme. No one needs that hassle.

(24) Does the department review P-Card transactions to look for unallowable or restricted purchases?[7]

Remember this sample checklist is from a state university. Like the government, there are certain costs that may not be charged to the government. If a government contractor wants to buy food and alcohol for a party, that is fine, but those costs better not find their way onto invoices to the government. Perhaps you have certain restrictions on what may be charged to the organization on a P-Card.

---

6 Ibid. p 3
7 Ibid. p 3

(25) Are actual expenses compared to budgets, and variations investigated?[8]

This control is not simply about the organization's performance. If the budget was put together based on recent history and anticipated changes in the market, variations may indicate that assumptions were mistaken, but the variations may also indicate fraud. The item below follows the same theme.

(26) Is general ledger verification performed monthly by departments and are unusual or unknown items investigated?[9]

Checking transactions each month may deter a would-be fraudster. Auditors will do the review. You can catch an oddity sooner doing the review right after the month-end, which is much better than doing it after year-end. Item 28 on this checklist takes this control a step further.

(28) As part of the GL verification process, is a sample of transactions under $500 selected to review for proper supporting documentation?[10]

This harkens back to the discussion of potential splitting transactions to get under the threshold. This control targets that threat. What would be "proper supporting documentation?" The requisition (request), the receiving report, and invoice all indicate the same amount, be it the amount of items or hours. Nowhere on an invoice is there a notation of shipping separately.

There are two items that address fraud awareness and reporting.

(31) Annually, are employees being alerted of new fraud schemes? [sic]

(32) Are your employees aware of the mechanism in place to report suspected fraud anonymously?[11]

The risk of the former is that some people may think, "What a great idea!" Nonetheless, it also has the advantage of implying, "We know the schemes that are being tried, and want you to know how to catch them before we do." Reminding everyone how to report suspected fraud never hurts and reminds someone thinking of scheming that others may report anything too odd.

Discussion question:

How do you think your personnel (co-workers) would take annual refreshers on fraud schemes and reporting "suspected" fraud? If negative, such as, "They think we're crooks", how can you mitigate the negative and turn the training into a positive?

In the early days of Sarbanes-Oxley training, your author did run into resistance. Most of it was in the form of "you don't trust us!" Be reassuring. You are not condemning your colleagues. You are giving them tools to prevent a scheme that could harm them. How? First, the damage to the organization's reputation

---

8 Ibid. p 3
9 Ibid. p 3
10 Ibid. p 3
11 Ibid. p 4

if customers or clients are defrauded may threaten the organization's viability. Second, even if the scheme is not against the customers or clients, the loss of money may cause other financial difficulties for the organization; in turn threatening raises, bonuses, or other morale-boosting activities.

III. Check-up

We highlighted a checklist utilized by the University of California San Francisco (UCSF) that included forty items for their various departments to check. Now we will look at a tool developed by the Association of Certified Fraud Examiners (ACFE), their *Fraud Prevention Check-Up*. It is very different from UCSF's. In fact, looking at the tool, there are only seven items. Rather than circle Y, N, DK, N/A, the ACFE wants you to score each item. The ACFE also recommends, "The check-up should ideally be a collaboration between objective, independent fraud specialists (such as CFEs) and people within the organization who have extensive knowledge about its operations."[12] [Parenthesis in original]

The first item I want to share here and get you thinking about is:

> **4. Fraud risk tolerance and risk management policy**
> To what extent has the organization identified and had approved by the board of directors its tolerance for different types of fraud risks? For example, some fraud risks may constitute a tolerable cost of doing business, while others may pose catastrophic risk of financial or reputational damage.
>
> To what extent has the organization identified and had approved by the board of directors a policy on how it will manage fraud risks? Such a policy should identify the risk owner responsible for managing fraud risks, what risks will be rejected (e.g., by declining certain business opportunities), what risks will be transferred to others through insurance or by contract, and what steps will be taken to manage the fraud risks that are retained. [Parenthesis in original]
>
> *Score from 0 (processes not in place) to 10 points (processes fully implemented, tested within the past year and working effectively).*[13] [Italics and parenthesis in original]
>
> These items appear in the left side column and in the right side are boxes to record "Results." At the bottom of the righthand column is a grey box to write the score.
>
> There are two critical words in the first part: tolerable and catastrophic. Crime has been rising in the United States, in some places more than others. One crime that seems to be more frequent is shoplifting. Back when your author was in retail, we tried to keep an eye on shoppers to prevent shoplifting. The problem was either real customers would require our attention, or the team would use one or more of their group to get our attention while other members shoplifted. In those days, it was the cost of doing business. It was, to an extent, tolerable.
>
> Now shoplifting appears to be rising to the level of catastrophic. The groups entering the store are larger and may not even try to be clever. These groups smash and grab, or simply dump items into trash bags to haul away. A store may be able to survive one of these incidents, but after a while, the cost of doing business is too high.

---

12 *ACFE Fraud Prevention Check-Up* Retrieved from https://acfe.com/fraud-resources/fraud-prevention-check-up on September 28, 2022 p. 4

13 Ibid. p. 6

Trying to transfer the risk to insurance companies may work for a while, but insurance companies are in business to make money. If the store can no longer get insurance, there is no choice but to shut down.

That is retail. What about other businesses and organizations? Think of your own. What fraud risks do you think are "the cost of doing business", and which are "catastrophic"?

5. The check-up moves to **Process-level anti-fraud controls and reengineering**. "To what extent has the organization implemented measures to eliminate or reduce through process reengineering each of the significant fraud risks identified in its risk assessment?"[14] The ACFE suggests that receipt of funds may be reengineered "by centralizing that function or outsourcing it to a bank's lockbox processing facility, where stronger controls can be more affordable."[15] This may also come with the cost of one, two, or more jobs, depending on how cash receipts are handled in your organization. It may also be an opportunity to reassign personnel where more help is needed. That is just one example.

Discussion question:

What opportunities may exist in your organization (or your clients' organizations) to reengineer internal controls to be more effective in both fraud prevention and financial reporting?

6. The next area in the check-up is **Environment-level anti-fraud controls**. This section is fascinating. It begins by discussing that major fraud occurs because senior managers can override controls simply due to their authority. The ACFE then notes that "soft" controls promoting appropriate workplace behavior are harder to implement than "hard" controls. Yet, the ACFE claims "they appear to be the best defense against fraud involving senior management."[16] This section takes up three pages, and we are not going to get into all of it. The key element is that promoting ethical behavior of staff rubs off on leadership. It may not totally eliminate "rules for thee but not for me", but it may give senior management a reason to think before acting – perhaps creating the difference between a catastrophic fraud and a "tolerable cost of doing business" fraud.

7. Proactive fraud detection

To what extent has the organization established a process to detect, investigate, and resolve potentially significant fraud? … Other measures can include audit "hooks" embedded in transaction processing systems that can flag suspicious transactions for investigation and/or approval prior to completion of processing. Leading-edge fraud detection methods include computerized email monitoring (where legally permitted) to identify use of certain phrases that might indicate planned or ongoing wrongdoing.[17]

These are proactive tests – such as running Benford's Law. There is one thing you will understand reading the whole checklist: it will not be completed quickly. Having a CFE assist may be worth the cost. Most likely you will be asked to provide your internal control documents, including the test results.

---

14 Ibid. p. 7
15 Ibid.
16 Ibid. p. 8
17 Ibid. p. 11

IV. Conclusion

There are many tools available to assess your controls. Take advantage of them. Fraud is occurring.

Summary

What a ride this was! We started with five fraud schemes that shocked the world, and there are many others we could have reviewed! What we know is that many who perpetrate a fraud scheme are smart. They may not believe they are perpetrating a fraud at first.

We then looked at groups of schemes and scams. Importantly, we made a distinction between a fraud scheme and a scam. The difference is the planned length. We stated that a *scam* is intended to steal someone's money once. Fraud *schemes* are intended to last for months or even years. We noted the three categories of fraud schemes: asset misappropriation, financial statements, and corruption. We then reviewed all the various schemes identified by the ACFE.

We did go over scams, though we did not really find any specific "internal controls" for them. However, we did note a fraud prevention checklist item that focused on annual training to make sure personnel were aware of phishing scams. In fact, most scams today start with a phishing email. We pointed out that by clicking on the sender's email we could find out more information, such as the actual email address. The long string will indicate that the email is fake. We emphasized that alerting friends and family could prevent losses. The one thing the scammers have in common is the desire to gain access to your computer. And we even discussed two YouTube channels to follow to watch the scammers get busted!

We made our way to reviewing various controls to detect and prevent fraud schemes. Some may be familiar to you. It is hoped that you have started thinking of ways to expand the use of these controls and the controls you already have in place at your organization (or your clients have in their organization).

After much discussion of controls, we reviewed two versions of a "checklist" to assess your internal controls. What was interesting was the two tools we found were different. One from the University of California San Francisco was forty items. The other from the ACFE was just seven items, but the associated text was much broader. The "check-up" as it is titled was meant to be used to guide discussion and inquiry. In fact, the ACFE suggests that we employ a certified fraud examiner in the exercise. This would be at least a day-long task, and it may be more than that.

Your author believes that if one can come away from any continuing professional education class with one new idea or insight, it was a worthwhile class. Hopefully, you had that experience.