# Fraud Case Studies: Schemes and Controls

FRD4/25/V1

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# This Product Is Intended To Serve Solely as an Aid in Continuing Professional Education

- Due to the constantly changing nature of the subject of the materials, this product is not appropriate to serve as the sole resource for any tax and accounting opinion or return position, and must be supplemented for such purposes with other current authoritative materials
- The information in this course has been carefully compiled from sources believed to be reliable, but its accuracy is not guaranteed
- In addition, Surgent McCoy CPE, LLC, its authors, and instructors are not engaged in rendering legal, accounting, or other professional services and will not be held liable for any actions or suits based on this manual or comments made during any presentation
- If legal advice or other expert assistance is required, seek the services of a competent professional

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Course Contents


- Chapter 1 – Introduction
- Chapter 2 – Five Schemes That Shocked the World
- Chapter 3 – Groups of Schemes and Scams
- Chapter 4 – Schemes and Scams
- Chapter 5 – Controls to Detect or Prevent Fraud
- Chapter 6 – Checklists and Assessments
- Chapter 7 – Summary

# A Quick Word on Policy vs. Politics

- Many times when discussing accounting, tax and finance policy issues, it can be difficult to divorce the politics from the policy
- Today, when discussing the various issues we will encounter over the next several hours, let’s agree to keep our own view of politics out of the application of the policy and focus on doing the very best we can for all our clients
- This goes for religious/faith views as well

# Chapter 1

# Introduction

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# 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

# Two Foundational Topics

- It is essential that we understand and appreciate two general topics:
  - Fraud victim organizations *have had controls in place*; and
  - There are reasons that good people go bad
- It is this foundation upon which we build

# Basic "Soft" Controls

- There have been as many as 18 controls in place
- We presume the controls were tested and deemed effective in design and operation
- But these are ***soft*** controls – it is difficult to gain concrete evidence they were being followed
- Fraudsters gladly sign a certification they have read the Code of Conduct and Ethics, or the financial statements are fairly stated in all material respects – that there is "no fraud or material errors"

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# What Is This Control?

- We will review those 18 controls and assess whether each control is “soft,” “evidentiary,” or both
  - A *soft* control has little or no hard evidence
  - A signed certification does not mean they **adhere** to the controls’ performance
  - Conversely, an *evidentiary* control has supporting documentation to provide some assurance – although documents may be faked

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# The ACFE 18 Controls in Place

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

# One Opinion

| 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 | |

# What Softens Controls?

- Internal Audit Department
  - Given *authority to perform the audit function*?
  - Are engagements planned and supervised?
  - Are the workpapers of high quality?
  - And you may want to add your own…

# This Also Goes For…

- External audits of financial statements and internal controls over financial reporting
  - Do they share peer review reports?
  - Do they permit their auditee liaison to discuss matters such as testing and reviewing – even for general understanding of what they are doing?
- And true for a dedicated fraud (prevention) department, function, or team
  - Who in the company has the capability to peruse their papers with understanding?

# But Wait – There's More!

- How do we assess the independence of audit committee members? (If you even know who they are!)
- Even a hotline or tipline is limited in effectiveness if action is not taken in a timely manner!
- Documentation of the investigation is critical to reaching a proper conclusion as to whether fraud occurred
- Let's look to the eponymous name in fraud…

# Charles Ponzi

- You’ve heard the name and know it’s some sort of investment scheme whereby early investors are paid a return, but later investors lose everything
- Do you know what Ponzi was selling?
- What was the investment opportunity he used to bilk so many people out of their money?



SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Ponzi Biographer Michael Zuckoff

- Journalism professor at Boston University writes that Ponzi was selling international reply coupons (IRC)
- An IRC is a form of voucher
  - Multiple countries accept them in exchange for local postage
  - Why would an IRC be valuable a century ago? Jets did not exist and there was no air mail
  - Sending letters overseas was expensive and slow
  - Ponzi could do nothing about speed, but he could make it less expensive…

# The Plan

- Ponzi visited Italy and realized he could buy 66 IRCs in Rome for the equivalent of one U.S. dollar ($1.00)
- The same number would have cost Ponzi $3.30!
  - Incidentally, as of February 2025, that is the equivalent of $32.09 (adjusted for inflation)
- Mail was the best way to communicate, especially over long distances
- Soon, Ponzi had thousands of people queued up to invest
- Technically legal, but practically impossible; as with any pyramid scheme, the shear weight was too much to bear the load

# Zuckoff's Real Motive

- The article's author not only wanted to tout his biography of Ponzi, but he also had a warning about a new potential Ponzi opportunity – cryptocurrency!
- Zuckoff said of crypto, "The good times roll, until they don't. This might sound like the stratospheric rise and recent plunge [(May 2022)] in values of the digital money known as cryptocurrency"

# What If…?

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

*See: 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

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# The Duck Test

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” *

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

# Not Again!

- Shortly after the first draft of this chapter, FTX collapsed
- Some $1 billion was unaccounted for by the end of 2022
- Allegations were that Sam Bankman-Fried (SBF) spent money on himself, friends, and family

# Fox News Digital Article

- December 11, 2022:

“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”

Not only does this article confirm we apparently do not own our own data… Venture capitalist Joe Lonsdale was blunt…

# Lonsdale

"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

# How Crypto Is Stored

- There is a great deal of high-level mathematics
- 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
- It is stored using a "pointer," which is attached to the Bitcoin file identifying the buyer using a password known only to the buyer

# Not Enough Memory

- Bitcoin was never meant to be used widely; the maximum file size is a mere one megabyte!
- Storage space is at a premium – look how many data centers have to be built!
- Remember when there was a run on Bitcoin and it shot up to $64,000? Early buyers did well, but Bitcoin did go down – Why?
- Space was needed
- The Data Miner must change the pointer from the seller to the buyer, and both pay a fee to the Data Miner! (See Mining Fees on page 1-5)

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Summary

- We have controls in place, but fraud can and does occur
- We may not be able to sufficiently test our "soft" controls
- We may not be able to sufficiently assess our auditors whether internal or external
- New schemes are being dreamed up using cryptocurrency and other devices
- Let's study five infamous cases

# Chapter 2

# Five Schemes That Shocked the World

# Learning Objectives

- Upon reviewing this chapter, the reader will be able to:
  - Understand the magnitude of the largest cases in recent years;
  - Understand the perpetrator(s) might be one person, or large groups; and
  - Recognize that some schemes could be spotted easily by a CPA

# Introduction

- We cannot cover all schemes that occur in a single year – there are too many!
- This section focuses on cases that, like December 7, 1941, live in infamy
- What is corporate fraud?

"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"

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Capital One Credit Card Data Breach

- The company's public statement:

"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"

- The hacker's name is Paige Thompson, former Amazon Web Services employee

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# The News

- The Good News: Capital One reported no credit card numbers, nor login credentials were compromised
- The Bad News: Around 140,000 Social Security numbers were obtained along with some 80,000 linked bank account numbers
- The company reported it had settled a lawsuit on April 22, 2022

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Why the Hack?

- What was in it for the hacker?
  - Social Security numbers are key to one's identity in the US
  - With those and linked bank accounts, the perpetrator could have sold the information for a lot of money; and/or
  - Hacked other sites and stolen identities

# Stolen Trade Secrets

- Again in 2019, the U.S. charged telecom company Huawei with several corporate and wire fraud schemes. The company is run by the Chinese Communist Party (CCP)
- Initial charges focused on Huawei lying about operating in Iran
- Huawei allegedly stole technology from T-Mobile (Recall the U.S. asked Canada to arrest Huawei's CFO)

# Why the Charges?

- The CCP/Chinese government wants to be the sole world superpower
- China is buying property in the U.S. – much of it, farmland – close to certain facilities
- If you work in an organization (or have clients) with sensitive trade secrets and business processes, employ strict controls on data systems

# Overseas Hijinks

- Go big, or go home – Steinhoff International is a South African, German, and Dutch international retail holding company
- Listed on both German and South African exchanges
- Founded in 1964 in Germany, it operates primarily furniture and household goods stores in Europe, Africa, Asia, Australia, New Zealand, and the US

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Something Was Up

- Steinhoff offices in Germany were first raided in 2015
- Two years later, share prices plunged upon word the company may have overstated profits and assets by nearly $12 billion
- It was a small group of executives who perpetrated the scheme before the Covid-19 pandemic
- Many brick and mortar retailers suffered and shuttered due to lockdowns; others survived with online business

# Please, Accept My Child

- Was there something in the water in 2019?
- Parents of students not particularly gifted in academics or athletics used bribes to get one or more child into noteworthy institutions, usually in cooperation with an athletic coach in low profile sports
- One prosecuting attorney said, “The real victims, in this case, are the hardworking students”
- Those students who were a better fit for the school and team were brushed aside

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Number Five

- What happens when the government provides a benefits program that grows to such a size that it becomes nearly unauditable? Fraud!
- Here's the scheme: "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 unnecessary for hundreds or thousands of elderly patients. The transactions were processed through call centers in the Philippines and Latin America

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Consider This

- How could an auditor who is not a medical professional assess whether something may be off?
  - 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
  - The estimated Fairfax County, Virginia population as of 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

# According to WebMD

- More than 50% of people over the age of 65 have some level of joint pain. How many need a brace?
- Let’s assume 40 percent of the patients 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 Wild Card – 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
- 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

# One For The Road

- 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

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# The 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 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

# Who Could Have Stopped It?

- 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”
  - If this pharmacy specialized in such medications, then perhaps it made sense

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# The Second Chance

- The second auditor is the one performing for the medical practice
- What if there was no audit required – just a tax return?
  - This is the best way 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 did not reveal how the scheme was uncovered, but money laundering is a leading candidate

# IRS Tools

- Information Returns Processing (IRP) System; it's simple!
  - The IRS matches information sent by employers and other third parties to the information provided by taxpayers
  - This includes taxpayer Forms W-2, 1099, and Schedules K-1
- Certain filters are also used to prevent fraudulent refunds for earned income tax credits (EITCs)
- We believe the IRS tracks information from other sources, including medical records, credit card transactions, and other electronic information
- Be careful what you post online!

# Such As…

- Expensive trips to Europe, Africa, even within North America!
- The IRS remains mum on the technique, but…
- The Electronic Communications Privacy Act permits federal law enforcement to view social media posts without a warrant (public domain)
- It includes emails stored longer than 180 days, as these are considered *abandoned*!
- And, of course, whistleblowers are used by the IRS

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# And Another Thing – Theranos

- The company was a medical testing device maker
- In 2003, 19-year-old Elizabeth Holmes was a freshman at Stanford University
- She believed she could make a collection pen akin to how a diabetes patient tests blood sugar levels
- She quit Stanford to start Theranos, convincing one of her professors (Channing Robertson) to be a board member
- Robertson connects Holmes with venture capitalists
- By the end of 2004 she has raised $6 million – and it's only a theory!

# Devil Is In The Details

- By 2014, Holmes was getting attention; the Food and Drug Administration approved the first test
- CFO Ramesh “Sunny” Balwani had no experience in biomedicine or technology start-up
- His fiery temper would earn him the title of company enforcer
- And by the way, Holmes and Balwani had a secret relationship kept from staff and the Board of Directors
- The mini-laboratory device named Edison would not work, and investors wanted some return, even losses

# Up Next

- An alert CPA, even CPA candidate, might have raised a warning
- Ask the question, “Who is getting this [bonus / payment / incentive]?
- Now we turn to see which controls ought to be in place to stop any fraud scheme quickly

# Chapter 3

# Groups of Schemes and Scams

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# 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

# Background

- We start with definitions
- There is an important distinction between *fraud* and *scam*, though some use the terms interchangeably
- We will use the definitions to ensure understanding

# Random House Dictionary

- **Fraud, noun**
  - **Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage**
  - The American Heritage Dictionary used “deliberately”; Random House seems to cover with “perpetrated”
  - Both dictionaries use virtually the same definition
  - **A particular instance of such deceit or trickery**
    - Mail fraud
  - **A person who makes deceitful pretenses; sham; poseur**

# The Next Key Word

- **Scam, noun; verb (used with object), scammed, scamming**
  - **(*Noun*) A confidence game or other fraudulent scheme, especially for making a quick profit; swindle**
  - You may know the key word in the definition by its abbreviated form – con game, con artist, and/or con man
  - The perpetrator gains the victim’s confidence, making the victim believe they have an advocate



SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Watch Words and Phrases

- They claim to be “a senior member of the fraud prevention team”
- A member of U.S. military “trying to get home for a wedding or funeral”
- They want to buy the lawnmower you have for sale, but you will need a PayPal account
- And the big one, “In order to assist you in this matter I will need you to download software” (Usually AnyDesk)

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# 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.”

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Critical Difference

- A fraud scheme is set up to syphon money over a long period of time – recall the average time of detection is typically between 12 and 18 months
- 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



SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Fraud Schemes – Types (Groups)

- Three types, or groups:
  1. Corruption;
  2. Asset Misappropriation; and
  3. Financial Statement Fraud

# Sub-Groups – Corruption

- The ACFE labels these:
  - Conflicts of Interest;
  - Bribery;
  - Illegal Gratuities; and
  - Economic Extortion
- Of the three main groups, this group is the smallest

# Sub-Groups – Financial Statement

- The ACFE labels two sub-groups – both focus on Net Worth and Net Income
- The only difference is whether net worth and/or net income is:
  - Overstated; or
  - Understated

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# The Largest Group

- Asset Misappropriation, which also has more subgroups than the others
- The ACFE breaks out two large asset misappropriation subgroups:
  - Cash and Inventory; and
  - All Other Assets
- The ACFE further breaks Cash into:
  - Theft of Cash on Hand;
  - Receipts; and
  - Fraudulent Disbursements

# Inventory and All Other Assets

- Misuse and Larceny, where the latter has additional schemes listed
- If you have the ACFE's *Occupational Fraud 2022: A Report to the Nations*, you will find a nice graphic on page 10, Figure 3

# Scams – Types

- Scams are initiated in two broad ways:
  - In-person communication; and
  - Phishing
- In-person may be by phone or by someone ringing the doorbell posing as a legitimate street vendor
- Scammers love the Internet. It allows them to:
  - Play on emotions (love and friendship);
  - Pretend to be a phony government official (tax debt due) or royalty in another country;
  - Portray your need to front money to claim a prize or product; or
  - Offer you an employment opportunity

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# How They Convince Victims

- Fraudsters and scammers share one common trait, they convince victims (marks) that they are honest and trustworthy
- Someone with the acting skills of any of the best actors on stage or screen, but with next to zero integrity
- We now dive into the schemes and scams within various types we have identified

# Chapter 4

# Schemes and Scams

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# 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

# ACFE's Fraud Tree

| | | |
|---|---|---|
| Asset Misappropriation | Financial Statement | Corruption |

# Asset Misappropriation

The ACFE identifies two categories of asset misappropriation:

- **Cash**
- **Inventory & All Other Assets**

# Cash

Theft of Cash On Hand

Theft of Cash Receipts

Fraudulent Disbursements

# Theft of Cash Receipts

- Cash Larceny
  - Snatching cash from the till or from colleagues when they are not looking and alert
- Skimming (Embezzlement)
  - Cash may be skimmed from sales, refunds, or receivables
  - Pilfer cash and never input sale
  - Fake refunds where there was never a sale
  - Phony receivables write-off, vendor never has to pay




SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Fraudulent Disbursements

- Billing Schemes – using shell companies
  - Company looks legitimate
  - Not really a going concern
- Non-Accomplice Vendor is a second victim
  - Vendor sends what the vendor believes is a proper invoice (think timesheet fraud, overbilling)
  - Both vendor and buyer thought the hours were worked, but not!
- Last, improperly billing for personal purchases

# Payroll Schemes

- Three schemes are tried and true:
  - Ghost employees;
  - Falsified wages; and
  - Commission schemes

# Expense Reimbursements

- Somewhat easier to pull off:
  - Mischaracterized expenses;
  - Fictitious expenses; and/or
  - Multiple reimbursements

# Check and Payment Tampering

- Check tampering is becoming obsolete
- Electronic fund transfers (EFT) through automated clearing house (ACH) fall victim to “tampering”
  - Someone alters recipient, amount, routing, and/or account number
  - Captures four schemes: forged maker, forged endorsement, altered payee, and authorized maker

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Inventory and All Other Assets

- The sub-category is **misuse** of the inventory and other assets
  - Company-owned and marked vehicle use to run personal errands
  - Internet usage
  - Personal calls/business on company phones
- **Larceny** of inventory and other assets
  - Includes unconcealed larceny, meaning we know something was stolen
  - An item is “shipped,” and an employee “receives”, though it never actually arrives




SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Financial Statement Fraud

Net Worth/Net Income Overstatements

Net Worth/Net Income Understatements

# Timing Difference

- Timing is everything, and it's why we use accrual accounting
- These schemes use timing to bend the truth
- Remember checking desk drawers for held accounts payable?

# Fictitious or Understated Revenue

- Motives differ:
  - Higher revenue to secure a loan; and
  - Lower revenue to lower taxable income
- Any journal entry made directly to revenue and equity without passing through the sales journal ought to be examined

# Liabilities and Expenses

- Either or both may be concealed, overstated, or understated (concealment)
  - Motives will vary:
  - Have beneficial financial ratios; or
  - Qualify for federal disaster relief

# Improper Valuation/Disclosures

- Auditors can be alert to the latter when reviewing final financial statements for signature
  - Perhaps guilt was getting to the signer(s)
- Valuation ought to be part of fieldwork
  - Allowance for doubtful accounts may be too low or too high
  - Inventory may be obsolete, and so forth

# Corruption

- Illegal Gratuities
- Economic Extortion
- Conflicts of Interest
- Bribery

# Which Schemes Are These?

- Conflicts of Interest
  - Purchasing schemes
  - Sales schemes
- Bribery
  - Invoice kickback
  - Bid rigging

# Bonus Schemes

- Some other schemes you may know:
  - Check kiting, though this is fading fast in the electronic era
  - Workers’ compensation fraud
  - Health insurance fraud
  - Product substitution
  - Data theft
  - Roundtrip transactions
  - Bill and hold
  - Up-front fees (popular scam, too)



SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Scams

- Typically geared toward getting cash and running – a quick hit:
  - Romance
  - Friendship
  - Facebook Friends
  - Distraught children/grandchildren (now using artificial intelligence!)
  - Prince/Government Official
  - Lottery/sweepstakes you never entered
  - Customs Clearance/Advance Fee
  - Internet Sale



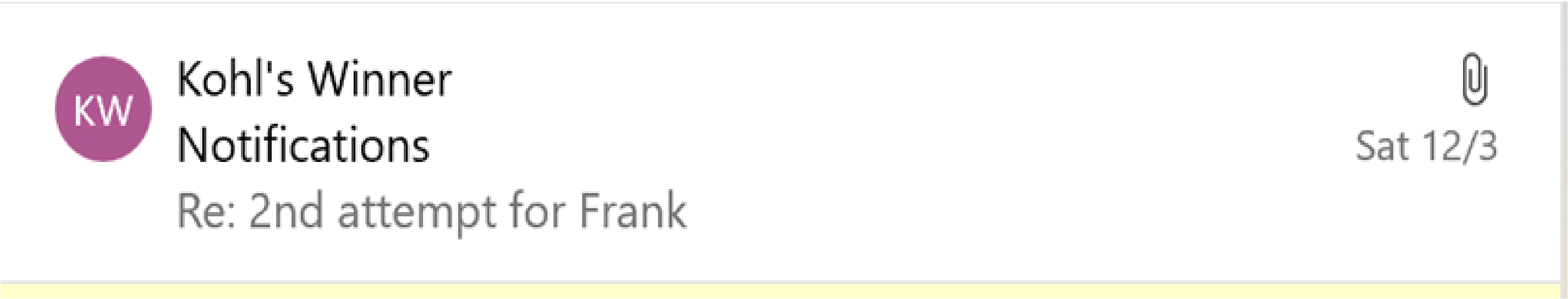

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Wait, There's More!

- Not done with the list yet (cont.)
  - Customs Clearance/Advance Fee
  - Internet Sale
  - Internet Loan
  - Internet Job

# An Email Scam

- Your author received this email:



# Here's The Body

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

27.17 KB

Re: 2nd attempt for Frank


SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# But…

- Right clicking on the Sender's name reveals the sender's email address and that the email is bait

KW

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

12/3/2022 10:23 PM

- These scams net $60 million a year!

# New Kid on the Block

- Corporate Transparency Act
  - Embedded in the National Defense Authorization Act enacted on New Year's Day 2021
  - Requires Beneficial Ownership Information (BOI) to be filed with Financial Crimes Enforcement Network (FinCEN) within U.S. Treasury Department
  - Fine for untimely filing is $500 a day!
- Scammers are already sending emails with URLs or QR codes
- FinCEN will not send unsolicited requests

SURGENT ACCOUNTING & FINANCIAL EDUCATION

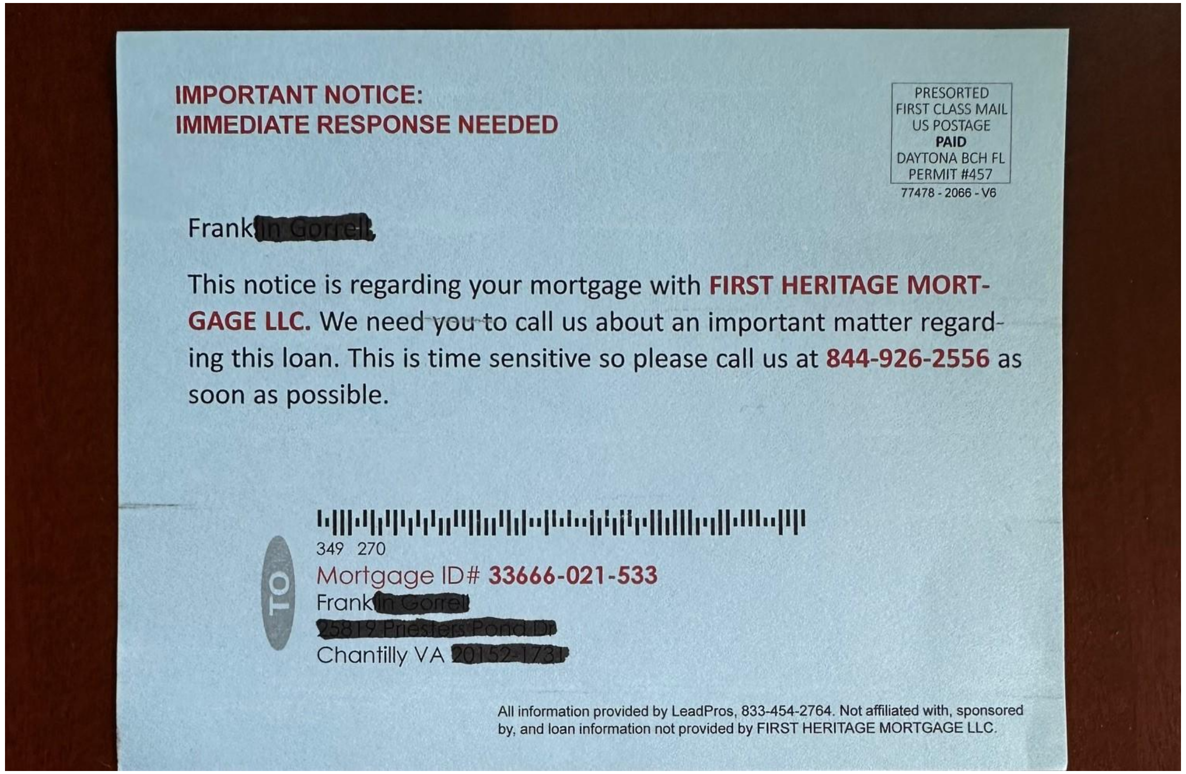
# Scammer Busters

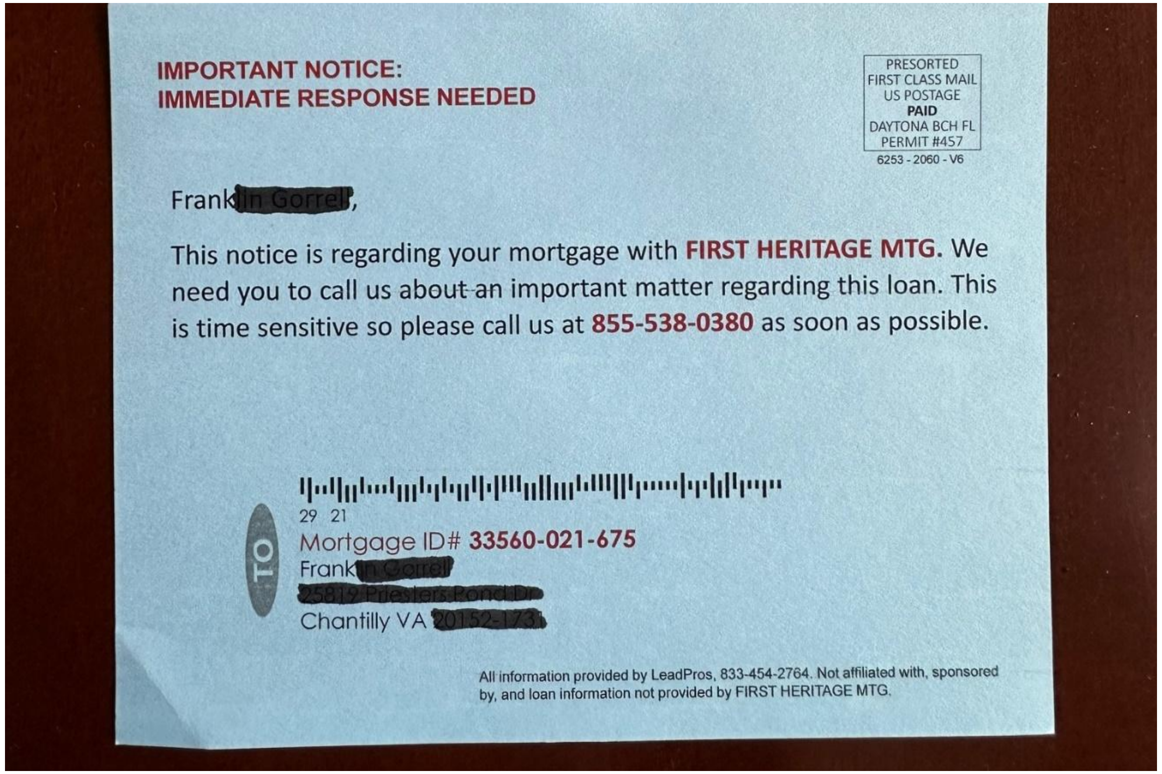
- Check out “Scammer Payback” a.k.a. “Pierogi” on YouTube
- Also on YouTube, Jim Browning – who trained Pierogi!
- They can reverse the connection and shut down scammers’ machines
- Browning even gets into their CCTV!
- Pierogi has been instrumental in having mules arrested

# Double Bonus

- Your author received two postcards just days apart:




SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Signs of a Scam

- Can you determine what may have tipped me off?
  - It refers to the company that issued the mortgage—not the present mortgage holder!
  - The holder’s name, the bar codes (and associated numbers), the mortgage identification, the telephone numbers, and the numbers under the postage mark were all different
- At least they had to keep the permit number

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Conclusion

- We've covered fraud schemes (long-term intent, mostly) and scams (short-term, one-time strikes)
- Stay informed
- Warn friends and family
- No reputable company will need to access YOUR computer to process a refund or credit
- If they want payment in Gift Cards – IT'S A SCAM!

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Chapter 5

# Controls to Detect or Prevent Fraud

# Learning Objectives

- Upon reviewing this chapter, the reader will be able to:
  - Understand that the groups of fraud schemes have certain key controls to prevent and detect fraud;
  - Understand the many ways 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

# Introduction

- Do you remember the conferences and seminars when Sarbanes-Oxley was new?
- The *number* of controls was a focal point – “Ten thousand controls!”
- Bit of an overstatement, as it often meant the company had 2,500 controls with key controls tested four times a year (2,500 x 4 = 10,000)
- Only 100 to 150 key controls were tested four times a year, which yielded 400 to 600 tests

# Consider

***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.)

# Asset Misappropriation

- Background checks
- Implement checks and balances
- Separate functions of preparer and signer
- Rotate duties of employees in accounts (receivable, payable, and other GL accounts)
- Delay commission payment until goods/services delivered and confirmed
- Keep checks locked up; destroy voided checks
- Conduct due diligence for new vendors
- Use data mining for anomalies and patterns

# Accounting Fraud

- Outside contractor performs regular reviews and reconciliations
- Mandatory vacation time
- Automated positive pay
- Reconcile balance sheet and payroll accounts quarterly
- Require managers or supervisors to approve timesheets and overtime claims

# Accounting Fraud – Concluded

- Restrict ability to modify pay rates and hours (at least two concurrences needed before changes)
- Perform data analytics
- Ensure terminated employees **are** removed from the payroll (meaning when final payment is made – for their work and any other leave to which they are entitled, there is no way that employee is paid via the payroll system)

# Foundation

- Corruption and bribery are very close, bribery may be limited to cash or some other item or favor of value
- Recall the movie *The Sting*: Paul Newman's character says, "The fix was in. The [police] took their cut…"
- Scammers in India bribe police, but folks like Browning and Pierogi are increasing pressure and embarrassment is building

# Corruption

- Strong code of ethics; “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”
  - This is the first of three interrelated controls
  - Training is critical
- Top levels set examples backing up the words in the code with actions

***Discussion question:***

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

# Fighting Corruption

- Discipline employees who breach the company's code of ethics
- Conduct due diligence on third parties with whom you do business
  - Consider that references offered are going to give a good reference
  - Check the Secretary of State's website for corporations to assess good standing and search officers' names for possible conflicts of interest; check the address; interview in person

# Product Substitution Red Flags

- Require high number of tests for parts and equipment acquired
- Assess if there is an unusually high number of repairs or replacements
- Lack of warranty information on the packaging
- Unbranded packaging
- Products do not look like the products ordered

# Corruption Concluded

- Conduct risk assessments for weak points
  - Internal control system
  - Morale
  - Processes with little or no back up controls or control performance cannot be confirmed
- Train all employees on bribery and corruption prevention
- Reward ethical behavior




SURGENT ACCOUNTING & FINANCIAL EDUCATION

# Data Theft

- Restrict access to proprietary information
- Set up IT controls to alert for certain activities
- Software alerts management of suspicious network activity
- Dispose of confidential information properly
- Use strong passwords to access sensitive data; consider additional authentication with a fob
- Clean desk policy

# In Conclusion

- We have reviewed some general controls
- Test your controls regularly and take nothing for granted
- Boost morale with group rewards and consider non-cash bonuses (money is nice, but a trip is priceless)
- Proactive training

# Chapter 6

# Checklists and Assessments

SURGENT ACCOUNTING & FINANCIAL EDUCATION

# 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

# Flowcharts

- Flowcharts seem to ebb and flow in popularity – there are times when flowcharts are all the rage, and other times when folks don't find them useful
- The advantage to flowcharting is ensuring we have the steps in the right order, and tying those steps and procedures to relevant controls
- Flowcharts also may reference other areas, such as Cash Receipts cross-referencing to Accounts Receivable or Human Resource's on- and off-boarding processes to Payroll

# Finding Gaps

- Suppose there are ten controls in a certain area, but only eight or nine are referenced in the flowchart. Is something missing? Seems to be
- If the flowchart indicates that all ten are included, and some steps in the process reference some more than once, it may indicate a strong internal environment
- Lest we forget, flowcharts are tailored to your needs; no one-size fits all

# Checklists

- Search the Internet, various checklists may be available
- Checklists are helpful tools – the movie *Apollo 13* shows many checklists, known as procedures; pilots use checklists for everything
- Ever forget something on the way to work? Maybe you need a checklist
- Great tool, but we still have to do the work

# Example

- The “Fraud Prevention Checklist” from the University of California, San Francisco is four pages long with 40 items
- On the top of the first page is this 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

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Key Words

**[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 there is the possibility, even probability, the system may weaken, and risk increase should anything change. Such as, 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."

# The Sections

- Four of the five sections are relevant to any organization:

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)
5. Sponsored Award Administration (Items 33 through 40)

# IT Controls/Cyber Security Critical Items

(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?

(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?

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

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Cash Receipts and Accounts Receivable Critical Items

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

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

# Cash Disbursements and Accounts Payable Critical Items

(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)?

- Good time to mention that dollar thresholds ought to be reviewed for the effects of inflation. What cost $1 in 2008 is about $1.41 today

# Cash Disbursements and Accounts Payable Critical Items

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

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

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

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

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Awareness Training 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? [sic]

- 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?

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Check-Up

- The ACFE *Fraud Prevention Check-Up*
- Different from UCSF's Yes, No, Don't Know, and N/A; the ACFE wants the user to score each item
- They recommend, "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"
- Let's look at two key items…

# 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)*. [Italics and parenthesis in original]




SURGENT ACCOUNTING & FINANCIAL EDUCATION

# 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.

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

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Chapter 7

# Summary

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Summary

- A lot of material
  - Five fraud schemes that shocked the world, and we could have reviewed dozens more
  - Fraudsters and scammers are smart, just using their skills for ill-gotten gains
  - We made a distinction between a fraud scheme and a scam; schemes are designed and intended for the long-term while scams are meant to be one-time hits for as much cash as possible

# ACFE's Fraud Scheme Tree

- There are three overall categories of fraud schemes:
  - Asset misappropriation;
  - Financial statement fraud; and
  - Corruption
- Within each of the categories are various specific schemes

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# The Scams

- We also discussed scams for two reasons
  - One is to alert you to the scammers’ attempts to make you a victim; and
  - Two, to help you protect those around you from being scammed. Note that older folks are primary targets of these scammers
  - Remember, anyone who states that direct access to your computer via AnyDesk or similar software is a scammer!
  - Don’t forget to look for Pierogi and Jim Browning on YouTube to learn more

# The Internal Controls

- There are controls that can detect and prevent fraud schemes
  - Most are familiar, such as code of ethics and approvals
  - Think of ways to expand controls already in place in your organization or your clients' organizations
- We covered checklists used in some organizations to assess various aspects of the systems; we touched upon the ACFE's checklist to assess your internal control environment

# In Conclusion

- If you have come away with at least one new idea or insight from this course, then it was a worthwhile four hours
- Final thoughts:
  - Review policies and procedures to ensure each reflects the actual current reality
  - Look to the release date and consider the impact of inflation on dollar thresholds




SURGENT
ACCOUNTING & FINANCIAL EDUCATION

# Thank you!

SURGENT
ACCOUNTING & FINANCIAL EDUCATION