



# Fraud Prevention:

The Prevention and Detection of Fraud Begins with You

# We're Glad You're Here!

- Please be sure you sign in!
- If you need Continuing Professional Education credits\*, this class qualifies!
  - Please check the box on the sign-in sheet. You will receive a CPE certificate from Audit Services in the following days.

\* The Office of Audit Services is an authorized provider of CPE through the Texas State Board of Public Accountancy.

# Takeaways

- What is fraud?
  - Definition
  - Facts
  - Four factors
- Fraud risk assessment
  - Two evaluation criteria
- Common fraud schemes
  - Case studies
- Prevention and detection controls
  - What can you do?



What is fraud?



# Definition

Fraud is any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

The Association of Certified Fraud Examiners

The American Institute of Certified Public Accountants

The Institute of Internal Auditors



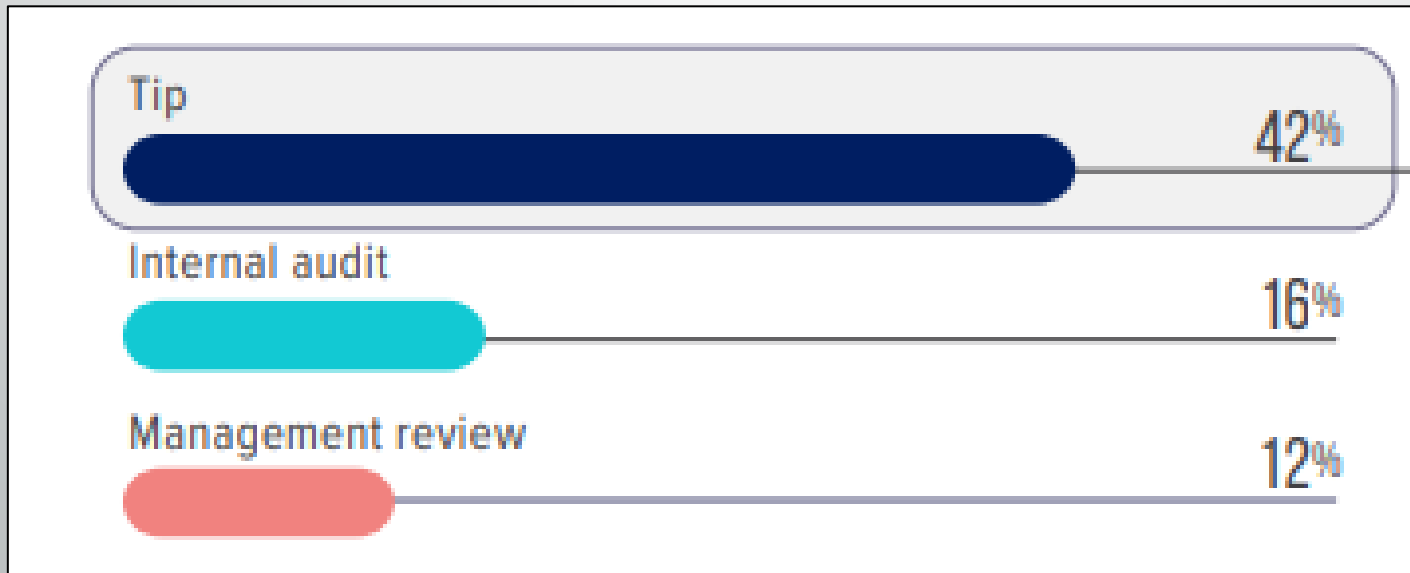
# Fraud Facts

The 2022 Report to the Nations on Occupational Fraud by the Association of Certified Fraud Examiners cited:

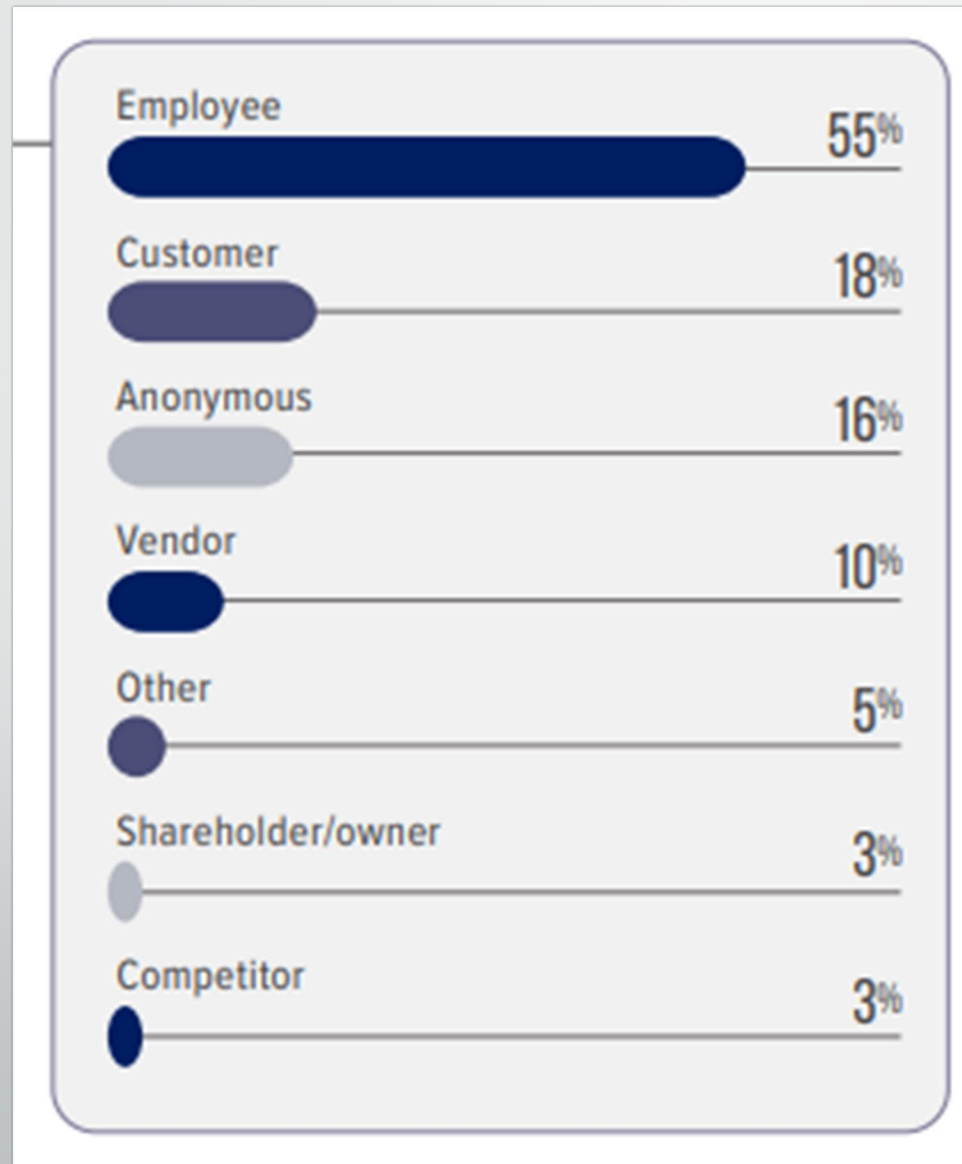
- The estimated typical organization loses 5% of revenues each year to fraud
- Operating budgets at Texas Tech University System are approximately \$2.5 billion, meaning \$125 million is at risk for fraud within the System!

# Fraud Facts

- In 2022, 54% of fraud cases were discovered by tips or during routine reviews by management.



# Sources of Tips



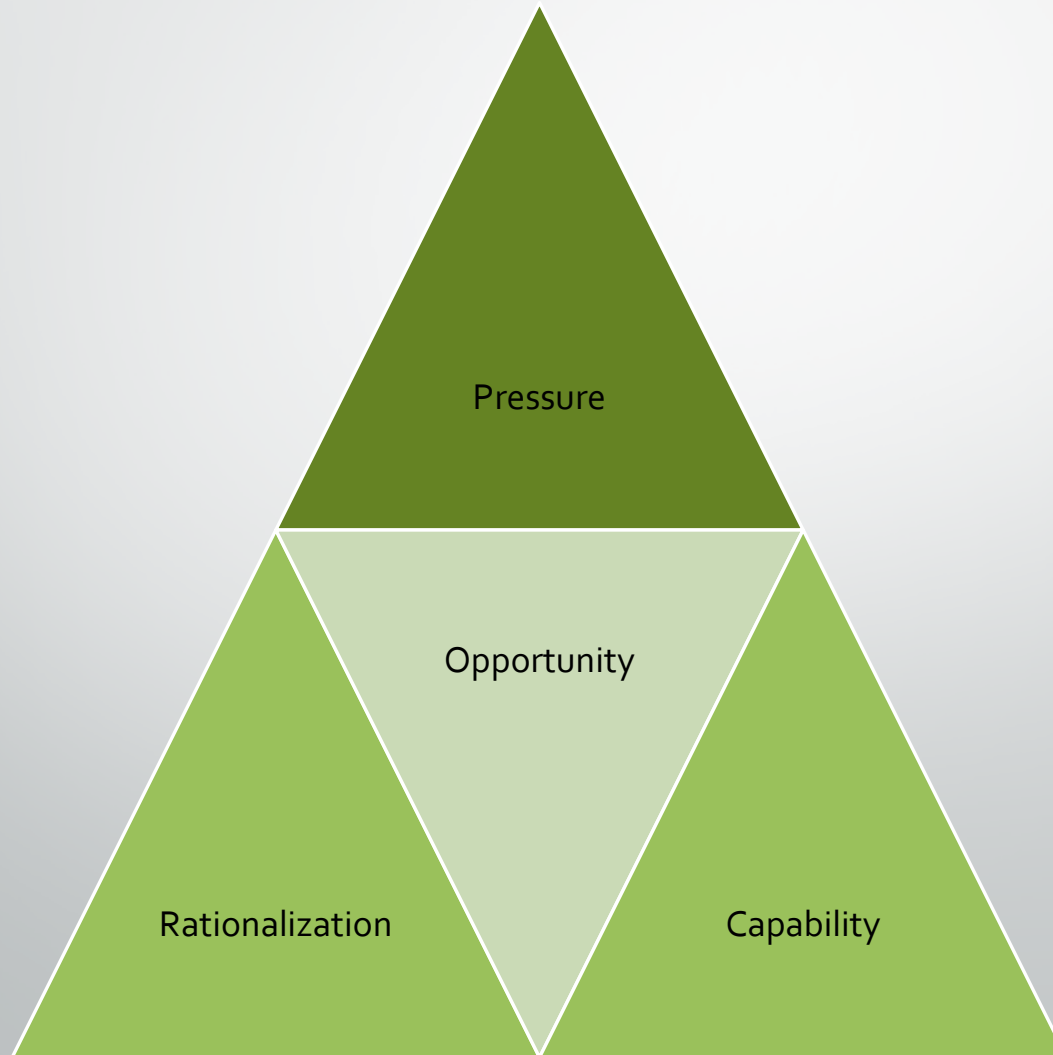




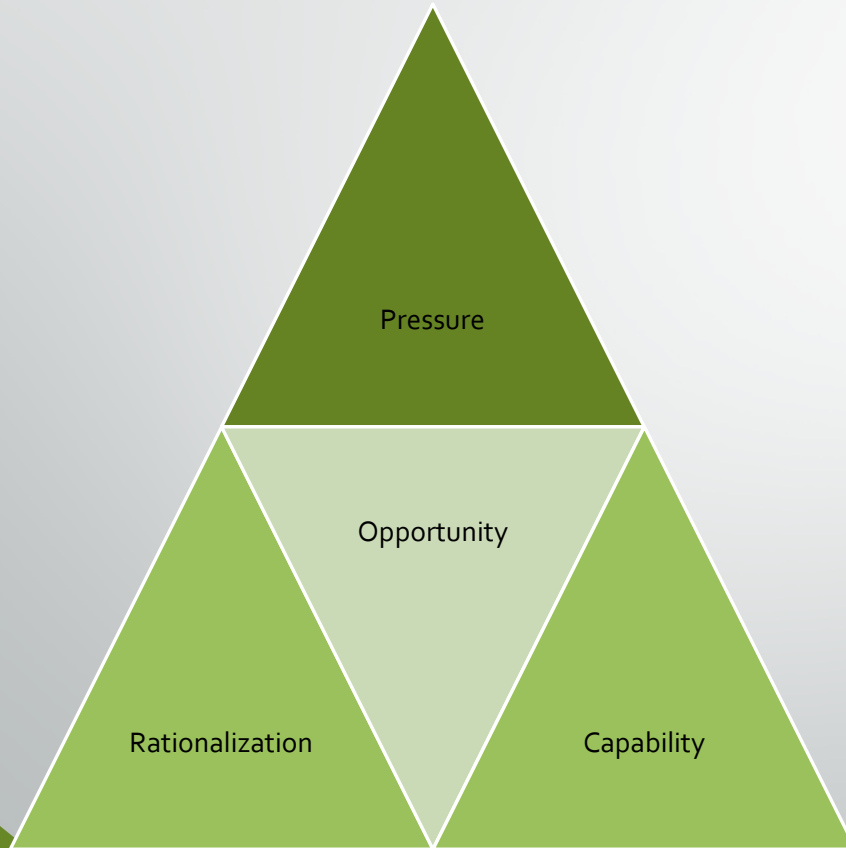
# Fraud Facts

- In 2022, 87% of fraudsters had no prior criminal history.
  - 13% did – thus, background checks
- In 2022, 83% of fraudsters had no prior employment issues related to fraud.
  - 17% did – thus, reference checks prior to hiring

# Four Fraud Factors

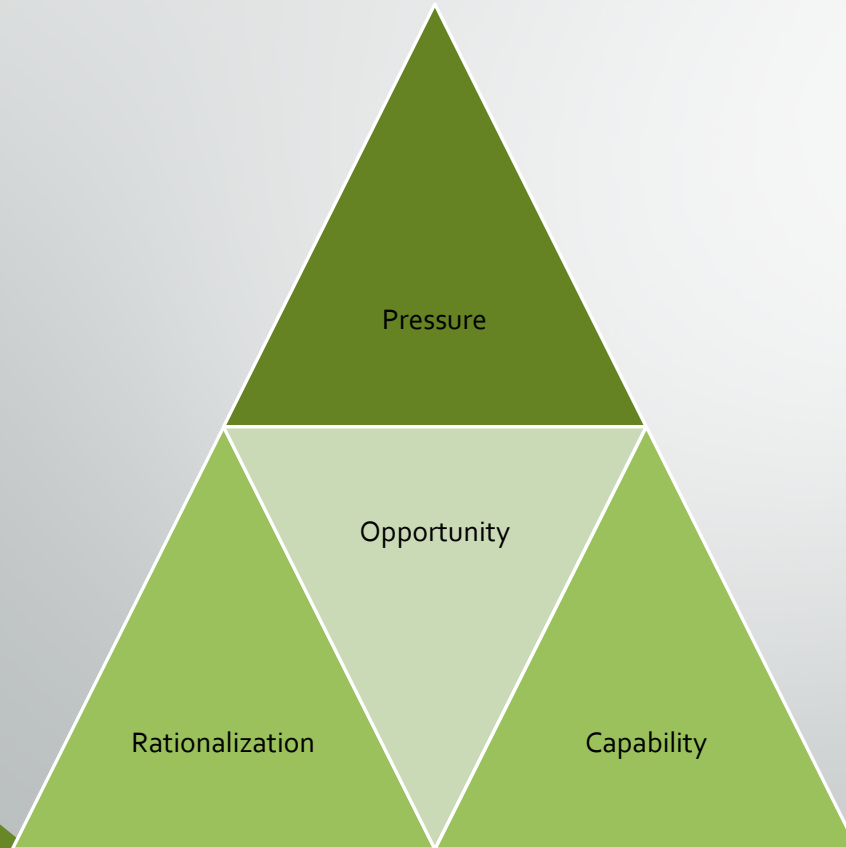


# Four Fraud Factors: Pressure



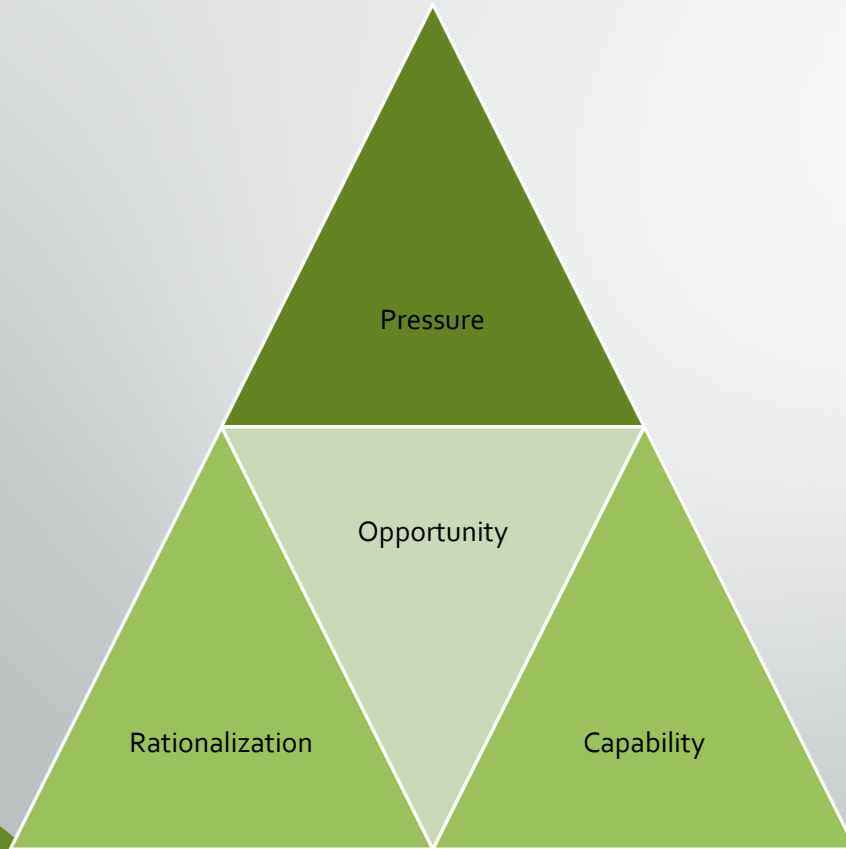
- Non-sharable financial pressure
- Family issues
- Gambling, alcohol, or drugs
- Overwhelming desire for financial gain
- Pressure to meet institutional goals
- Dissatisfaction at work

# Four Fraud Factors: Capability



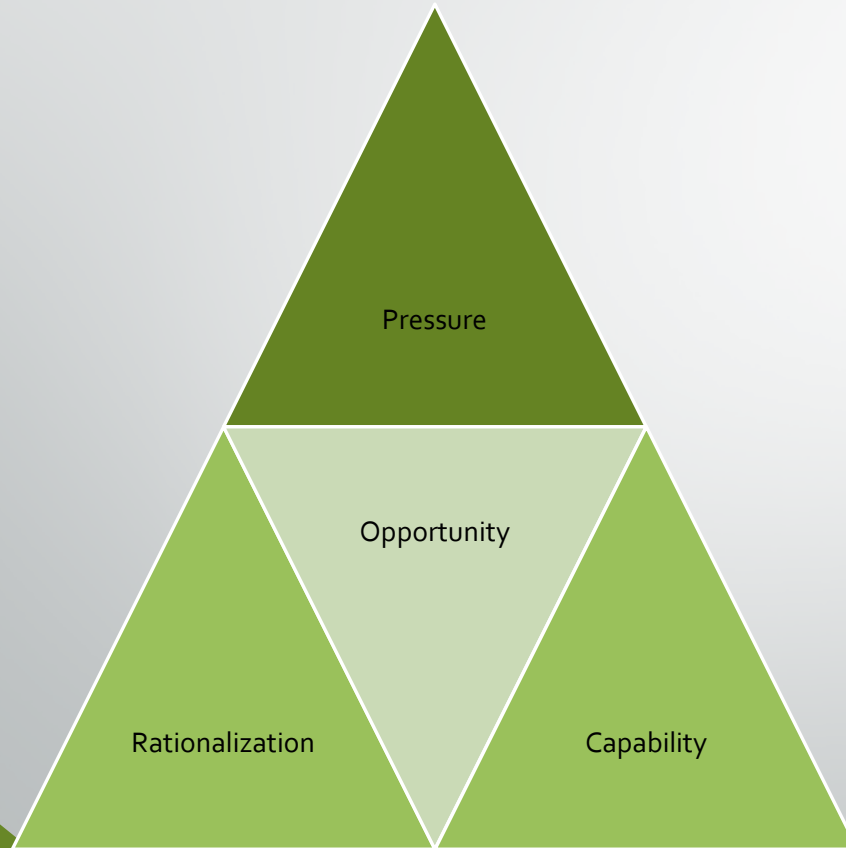
- Position or function within the organization
- Personal traits and abilities
- Confidence in one's ability to commit fraud undetected
- Ability to talk one's way out of trouble
- Deals well with stress

# Four Fraud Factors: Rationalization



- A way to justify in the person's consciousness that the act of fraud is not so bad
- Common beliefs:
  - Person is owed this money
  - Just borrowing until they are able to pay it back
  - Everyone else is doing it

# Four Fraud Factors: Opportunity



The only aspect the organization really controls is opportunity.



# Fraud Risk Assessment



# Fraud Risk Assessment

- A fraud risk assessment identifies where fraud may occur within the organization.
- A fraud risk assessment should:
  - Consider relevant fraud schemes and scenarios
  - Map those schemes and scenarios to mitigating controls



# Two Evaluation Criteria

## 1. Likelihood

- What is the probability that this type of fraud will occur at our institution?

## 2. Pervasiveness

- Assuming that this type of fraud could occur or is occurring, would it affect only a few division/departments or is it something that could be widespread?

A decorative graphic on the left side of the slide, consisting of several overlapping, parallel lines in shades of green and grey, forming a stylized, angular shape that points towards the center.

# Common Fraud Schemes



# Common Fraud Schemes

## Asset Misappropriation

- Cash Theft
- Inventory and Other Assets
- Fraudulent Disbursements
  - Billing schemes
  - Expense reimbursement schemes
  - Check tampering
  - Payroll schemes

## Corruption

- Conflicts of Interest
- Bribery and Incentives
- Information Technology



# Asset Misappropriation: Cash

## Larceny

- Theft of cash receipts or cash on hand
  - Reversing transactions
    - False refunds / voids
  - Altering cash counts
- Theft of cash from the deposit
  - Deposit lapping



# Case Study: TTUHSC Amarillo Business Office

Schemes: Theft of Cash, Receivables Lapping, Deposit Lapping

- Lack of segregation of duties in cash handling, payment posting, and deposit processes
- No supervisory review or approval of deposits
- Cashier stole over \$535,000 in cash from deposits over an 8-year period.



# Asset Misappropriation: Cash

Skimming: Theft before a transaction is recorded in an accounting or cash system

- Point-of-sale skimming
  - “If you do not receive a receipt, notify a manager! Your next meal is free!”
- Accounts receivable skimming
  - Forcing account balances or destroying transaction records
  - Lapping
  - Writing off account balances
    - Discounts or Allowances



# Fraud Prevention: Cash Theft

## Red flags:

- Cash is missing!
- One person does it all
- Deposits are not made timely
- Patient or customer complaints
- High discounts, refunds, voids, or write-offs
- Cash often out of balance

# Fraud Prevention: Cash Theft

What to monitor:

- Segregation of duties
  - Custody
  - Recording
  - Reconciliation
- Surprise cash counts
- Refusal to take time off
- Detailed reconciliation of monthly ledgers






# Asset Misappropriation: Inventory and Other Assets

## Inventory and Other Asset Misappropriation


- Misuse
  - Any use that is not associated with the University's intended or expressed used of the asset
- Larceny
  - Purchasing and receiving schemes
  - Asset requisitions and transfers



# Case Study: TTUHSC Lubbock Correctional Managed Healthcare

Scheme: Inventory misappropriation

- Material Manager purchased large amounts of medical equipment with University funds and sold medical equipment through personal eBay and Amazon accounts
- Type of equipment was reasonable, but volume was excessive
- Questionable purchases totaled over \$580,000 over a 5-year time period




# Fraud Prevention: Inventory and Other Assets

## Red flags:

- Missing equipment, supplies, etc.
- Excessive purchases
- Attitude of “It’s Mine”
- Items shipped to non-institutional addresses

## What to monitor

- Know what is “normal”
- Segregation of duties in ordering / receiving / bill payment
- Tracking of risky inventory (i.e. iPads, laptops)
- Purchases from certain vendors: Amazon, eBay, Walmart



# Asset Misappropriation: Fraudulent Disbursements


## Billing schemes

- Shell companies
- False invoicing
- Personal purchases with institutional funds

# Case Study: TTU Housing

## Scheme: Shell Company Billing Scheme

- Employee created a shell company between the University and the legitimate vendor – a tile layer
- Instructed the vendor to bill the shell company
- Shell company billed the University for double the actual cost
- The University paid \$281,920 to the shell company over 1 ½ years




# Fraud Prevention: Billing Schemes

## Red flags:

- Invoices slightly below bid limits
- Over-concerned or interested parties
- Sketchy vendor information

## What to monitor


- Multiple payments across several invoices exceed bid limits
- Consecutive invoice numbers
- Generic invoices
- “Smell test”: something just doesn’t seem right



# Case Study: TTUHSC El Paso Center of Excellence in Cancer

## Scheme: Billing Scheme – Personal Purchases

- Abuse of purchasing authority by fund manager
- Lack of segregation of duties in purchasing process
- 175 items (approximately \$8,600) over an 8-month period that appeared to be personal or non-work related
- Pressure to spend down state funds



# Fraud Prevention: Personal Purchases


## Red flags:

- Overpurchasing
- Unusually high number of P-Card transactions
- Duplicate purchases on P-Cards on the same approximate date, time, and amount
- Purchasing of items through non-TechBuy vendors

## What to monitor:

- P-Card statements, card sharing, and logs
- eRaider approvals
  - DO NOT share your eRaider / Banner passwords with ANYONE.






# Asset Misappropriation: Fraudulent Disbursements

## Expense reimbursement schemes


- The most common disbursement frauds are:
  - Mischaracterized expense reimbursements
  - Fictitious expense reimbursements
  - Overstated expense reimbursements
    - Altered receipts
    - Overpurchasing
  - Multiple reimbursements



# Case Study: TTU Student Financial Aid

## Scheme: Mischaracterized Expense

- Student Financial Aid employee submitted travel voucher for recruiting event over Memorial Day weekend
- Employee could not remember details or provide documentation of event
- Purpose of trip on voucher was vague




# Fraud Prevention: Expense Reimbursement

## Red flags:

- Fuzzy support / details
- Missing, altered, generic, or non-original receipts

## What to monitor:

- Detailed expense reports should include:
  - Original receipts or other supporting documentation
  - Specific business purpose
  - Date, place, and amount



# Asset Misappropriation: Fraudulent Disbursements

## Check tampering schemes

- Forged maker
- Forged endorsement
- Altered payee



# Case Study: TTUHSC Lubbock SIMLife Center

Scheme: Theft of Cash, Check Tampering, and Billing Scheme – Personal Purchases

- Two employees directed customers to pay with cash or leave checks blank
- No cash deposited
- Over \$20,000 in cash and checks may have been stolen over a 1-year time period
- One employee gave her eRaider name and password to her son to set up carts in TechBuy


# Fraud Prevention: Check Tampering

## Red flags:

- Missing cash or deposits
- Customer or patient complaints

## What to monitor:

- Lock up the check stock / check book
- Segregation of duties
- Surprise cash counts
- Reconcile your monthly ledgers



# Asset Misappropriation: Fraudulent Disbursements

## Payroll schemes

- Falsification of a timecard or information in the payroll records
- The most common payroll frauds are:
  - Falsified hours
  - Ghost employees




# Case Study: Angelo State Timesheet Fraud

## Scheme: Payroll – Falsified Timesheets

- Student Assistant reported 333 hours that she did not work over a 6-month time period, resulting in overpayments of \$2,600
- Timesheet approver did not know actual hours worked
- Theft of time is still fraud





# Fraud Prevention: Payroll

## Red flags:

- Blaming the system for pay errors
- Overrides on the time clock
- Unknown employee in pay records

## What to monitor:

- Reconcile monthly account ledgers
- Approval of timesheets



# Corruption: Conflicts of Interest

## Types of Conflicts of Interest


- Purchase schemes
- Entitlement schemes
- Conflicts of commitment



# Case Study: TTUHSC El Paso Storage Facility

## Scheme: Conflict of Interest – Purchase

- Director of Facilities Department had conflicts of interests with several vendors used by the department
- Director leased a storage facility owned by his son
- Facilities paid \$116,000 to these vendors over a 9-year time period, \$100,000 of which was to his son



# Case Study: TTU College of Agriculture

Scheme: Conflict of Interest – Purchase and Entitlement

- Tenured professor awarded over \$15,000 in scholarships to his children and \$7,500 to his son's girlfriend
- Purchased livestock from his minor children
- Culture of department resulted in multiple issues over a 9-year period



# Fraud Prevention: Conflicts of Interest

## Red flags:

- Tips and complaints
- Favorable treatment of a certain vendor
- Unusual request for influence
- Inflated prices

## What to monitor:

- Conflict of interest disclosures
- Procurement process violations
  - POs after the fact
  - No segregation—one person makes all the decisions
  - Other possible vendors not given appropriate consideration



# Corruption: Bribery and Incentives

## Types of Bribery and Incentives Schemes

- Bid-rigging schemes
  - “Need” recognition
  - Specifications
- Bribery schemes
  - Kickbacks



# Case Study: TTU Athletics Sports Nutrition

## Scheme: Conflict of Interest – Bid Rigging

- No segregation of duties in purchasing and inventory processes
- Director of Sports Nutrition Program owned company used to purchase supplements
- Athletics purchased over \$430,000 of supplements over a 2-year time period

# Fraud Prevention: Bribery and Incentives

## Red flags:

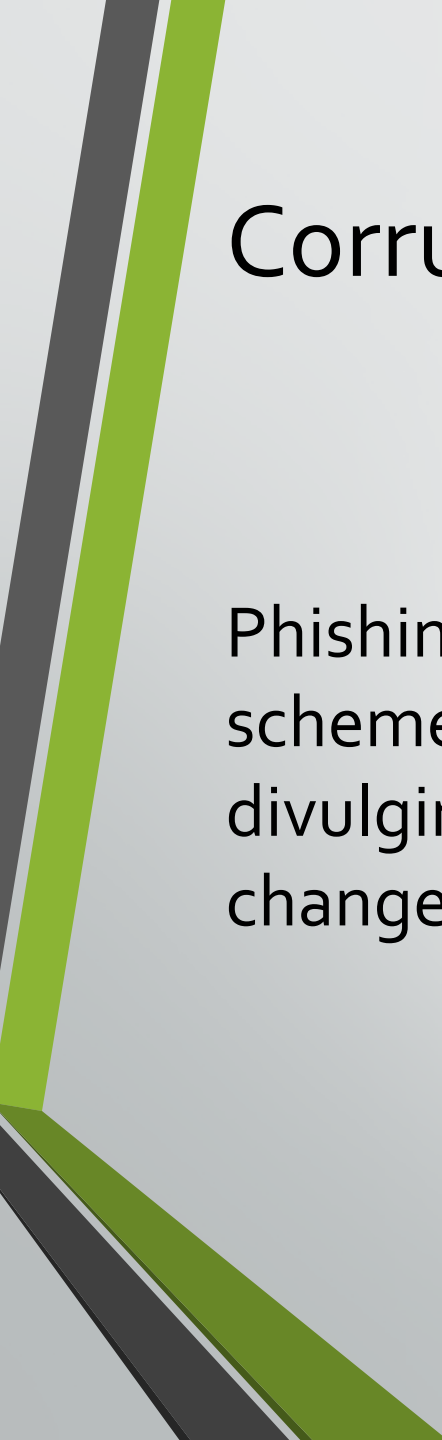
- Gifts and favors
- Favorable treatment of a certain vendor
- Using an unusual or non-contract vendor
- A person who insists on being the point of contact
- Paying a higher price
- A constant vocal complainer



# Fraud Prevention: Bribery and Incentives

What to monitor:

- Market value of products purchased
- Higher than expected volume of purchases from particular vendors
- Unnecessary purchases



# Corruption: Information Technology Schemes


Phishing is a type of information technology scheme where fraudsters trick individuals into divulging information or making unauthorized changes to information.



# Case Study: TTUHSC Purchasing

## Schemes: Cash Misappropriation and Phishing


- Phishing scheme used to convince vendor set-up team to change vendor bank account information
- Payments totaling \$818,000 intended for Western Builders were diverted to a fraudster's bank account
- Insurance denied the claim because the vendor set-up team member violated policy



# Fraud Prevention: Phishing Schemes

## Red flags:

- Anyone asking for your login ID or password
- An unwarranted sense of urgency
- Errors or irregularities in emails or written correspondence
- Multiple calls with no voicemail
- Email subjects such as "Your mailbox is almost full" or "Account Closure Verify Now"
- Switching information or accounts from local to something in another state or country



# Fraud Prevention: What can I do?

## Ensure proper segregation of responsibilities

- No one person should have control of any process: purchasing, p-card, payroll, HR, cash handling
- NO password sharing

## Reconcile your FOPs monthly

- Conducted by a person not in the procurement process, if possible

## Review procurement card statements, including receipts

- Do not simply sign them and pass them through

## Review approval authorities

- Limit the number of individuals with approver or requestor authority on FOPs
- Ensure only current employees have access
- Conduct the review no less than annually

## Review travel documents, including receipts

- Do not simply sign them electronically and pass them on

## Count inventories regularly

- Conduct a count of inventory and compare to inventory amounts in tracking systems

## Conduct surprise cash counts

- Stress that it isn't distrust of the employee, but is a routine responsibility in cash handling areas

## Pay attention to details in email/phone communications

- Don't respond to fishy (phishing) requests
- Notify IT immediately if your department falls prey

## ASK QUESTIONS

- No one has unquestioned authority to do as they wish



# Reporting Fraud

If you suspect fraud:

- Report it to your supervisor, University Police, or General Counsel
- Contact the Office of Audit Services by phone
  - TTU: 806-742-3220
  - HSC: 806-742-3220
  - ASU: 325-942-2261
  - HSC El Paso: 915-215-4148
  - MSU: 940-397-4914
- Report your suspicions anonymously at [www.ethicspoint.com](http://www.ethicspoint.com)



# Presentation Resources and Works Cited

- 2020 ACFE Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners.
- Managing the Business Risk of Fraud: A Practical Guide, ACFE, AICPA, IIA, 2007.
- Principles of Fraud Examination. Joseph T. Wells. 2005.
- 2007 Fraud Examiner's Manual, ACFE, 2007.
- The Fraud Diamond: Considering the Four Elements of Fraud. David T. Wolfe and Dana R. Hermanson. 2004



# Fraud Prevention

It Starts with You!