



Overview of Fraud Prevention and Detection

The Prevention and Detection of Fraud
Begins with You

Niki Countryman CPA, CIA, CMA, CFE
Senior Internal Auditor
System Office of Audit and Consulting Services



Learning Objectives

- What is Fraud?
 - Definition
 - Facts
 - Four Factors
- Common Fraud Schemes
 - Scenarios
- Prevention and Detection controls
 - What can you do?
- Resources

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.

Association of Certified Fraud Examiners
The American Institute of Certified Public Accountants
The Institute of Internal Auditors

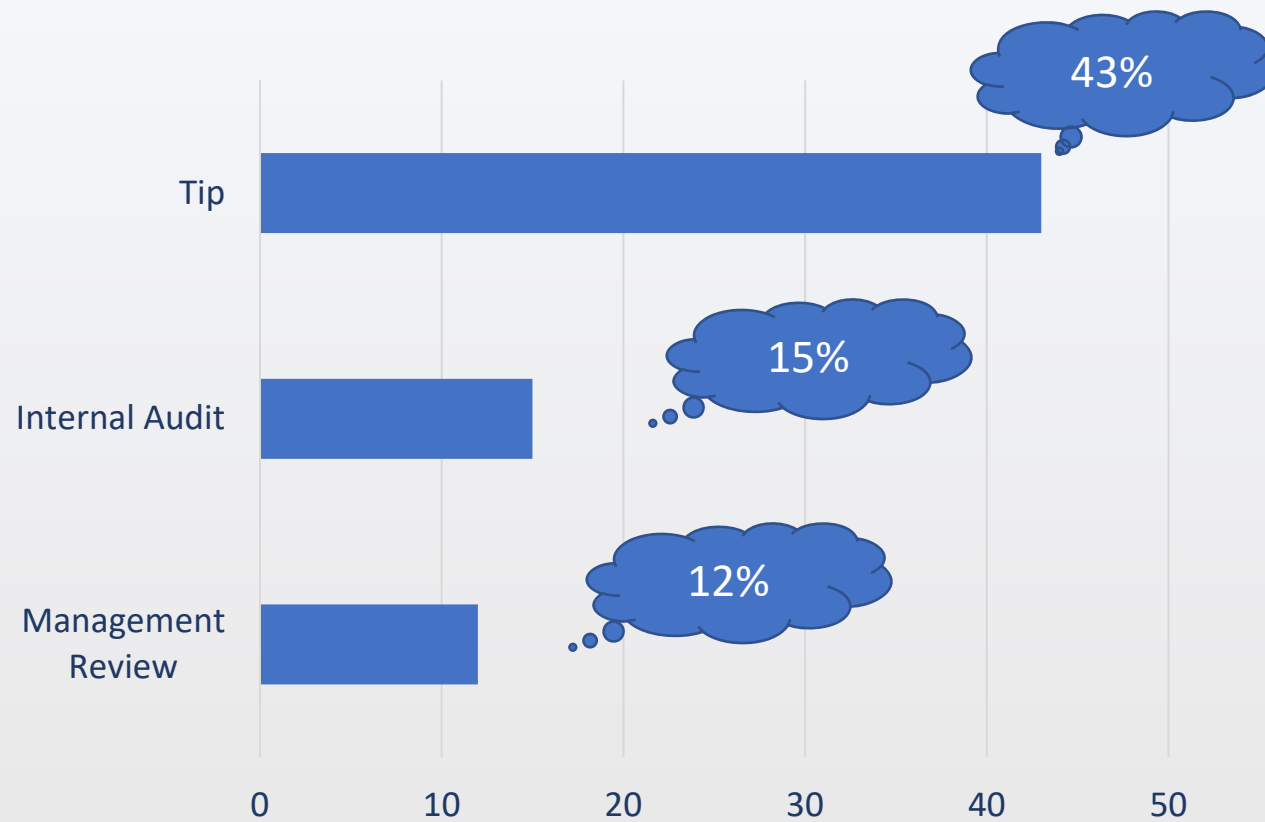
The Cost of Fraud

- Fraud costs a typical organization an estimated 5% of its annual revenue
- Revenues at the University of Alaska in 2020 were over \$711 million, 5% of which would be \$35 million!

ACFE, 2020 Report to the Nations
FY20 UA Audited Financial Statements

Fraud Facts

In 2020, 43% of fraud cases were discovered by tips or during routine reviews by management.



ACFE, 2020 Report to the Nations

5

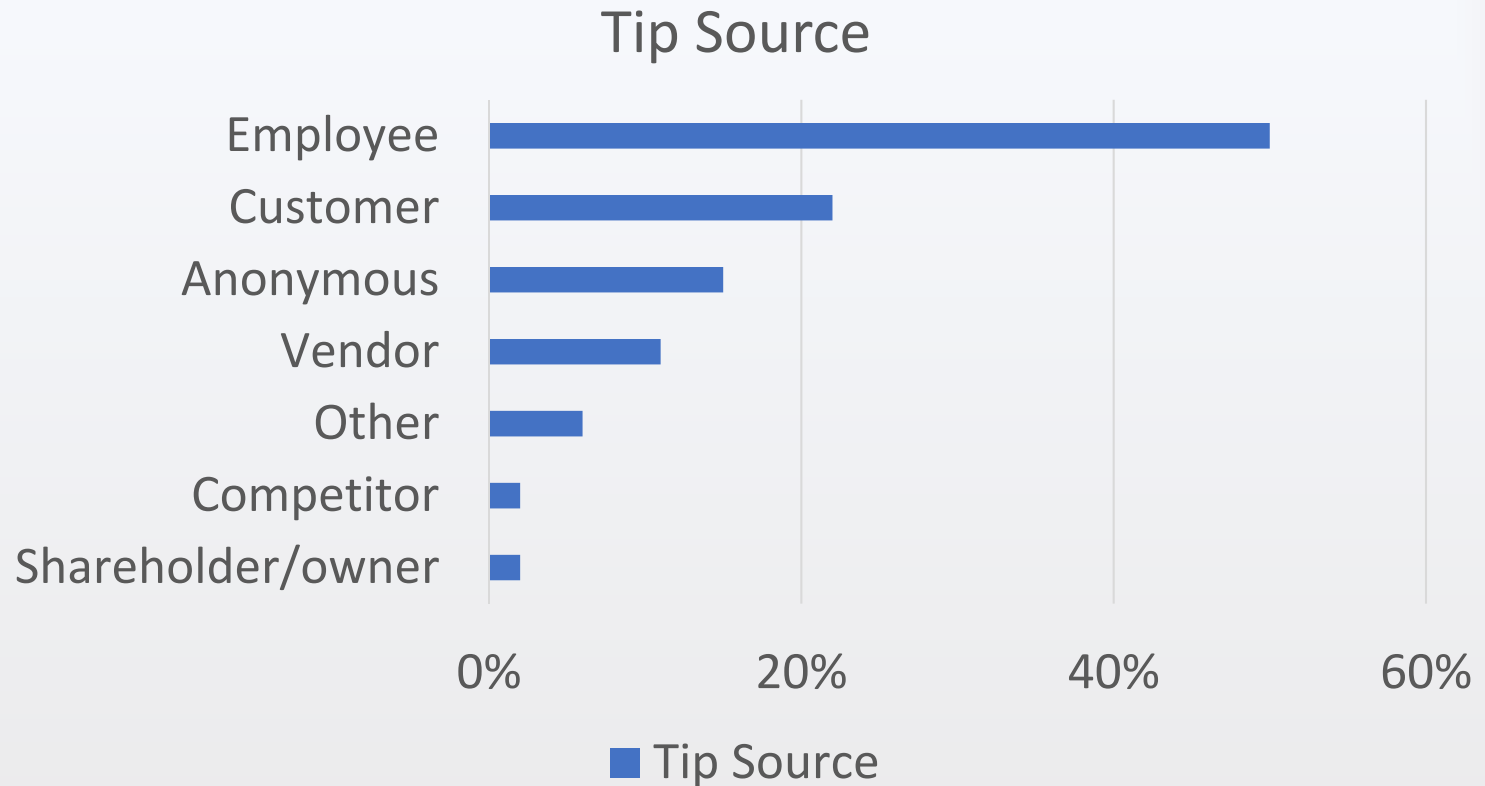
Fraud Facts

How is occupational fraud initial detected?

<u>Detection Method</u>	<u>Percentage of Cases</u>
• Tip	43%
• Internal Audit	15%
• Management Review	12%
• Account Reconciliation	6.1%
• Document Examination	4.8%
• External Audit	4.0%
• Surveillance/Monitoring	1.9%
• IT Controls	1.5%
• Other	16.3%

Association of Certified Fraud Examiners
2020 Report to the Nations

Fraud Facts



Association of Certified Fraud Examiners
2020 Report to the Nations



Identify the Fraudster



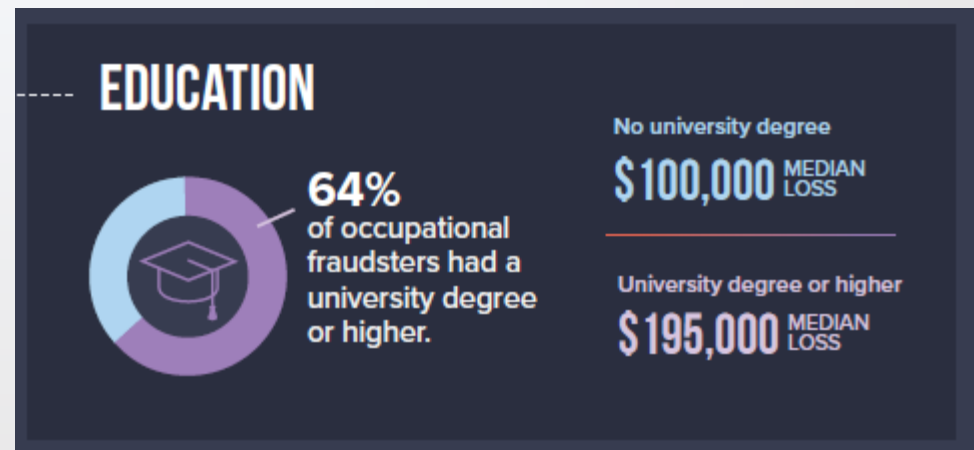
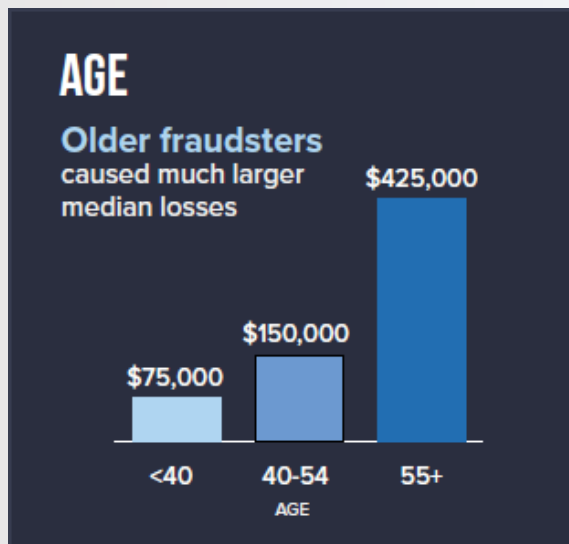
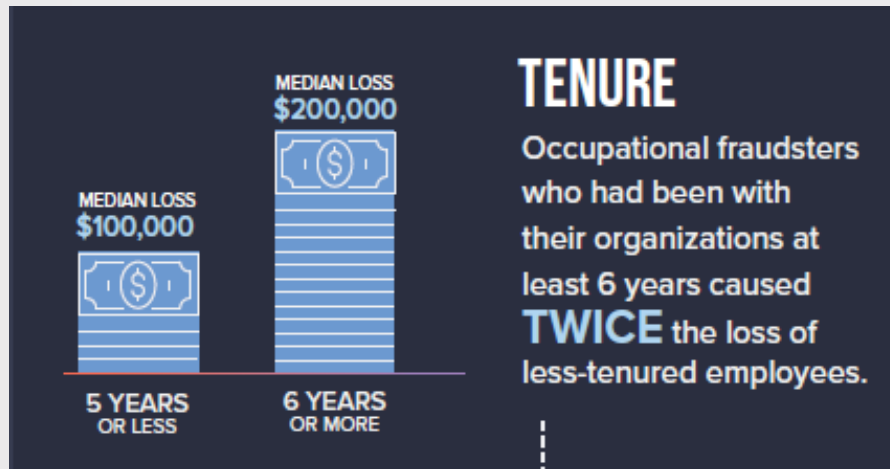
UNIVERSITY
of ALASKA
Many Traditions One Alaska

Identify the Fraudster

If you want to know what a fraudster looks like, look to the person on your right, then to the one on you left, and it will look like the person in the middle. White-collar criminals look like you and me.

Jeff Matthews

Profile of a Fraudster



Profile of a Fraudster

- In 2020, 89% of fraudsters had no prior criminal history.
 - 11% did – thus, background checks
- In 2020, 86% of fraudsters had no prior employment issues related to fraud.
 - 16% did – thus, reference checks prior to hiring are important

*Association of Certified Fraud Examiners
2020 Report to the Nations*

Profile of a Fraudster



MORE THAN HALF of all occupational frauds came from these four departments:



OPERATIONS 15%



ACCOUNTING 14%



EXECUTIVE/UPPER MANAGEMENT 12%



SALES 11%

EDUCATION



64% of occupational fraudsters had a university degree or higher.

No university degree

\$100,000 MEDIAN LOSS

University degree or higher

\$195,000 MEDIAN LOSS

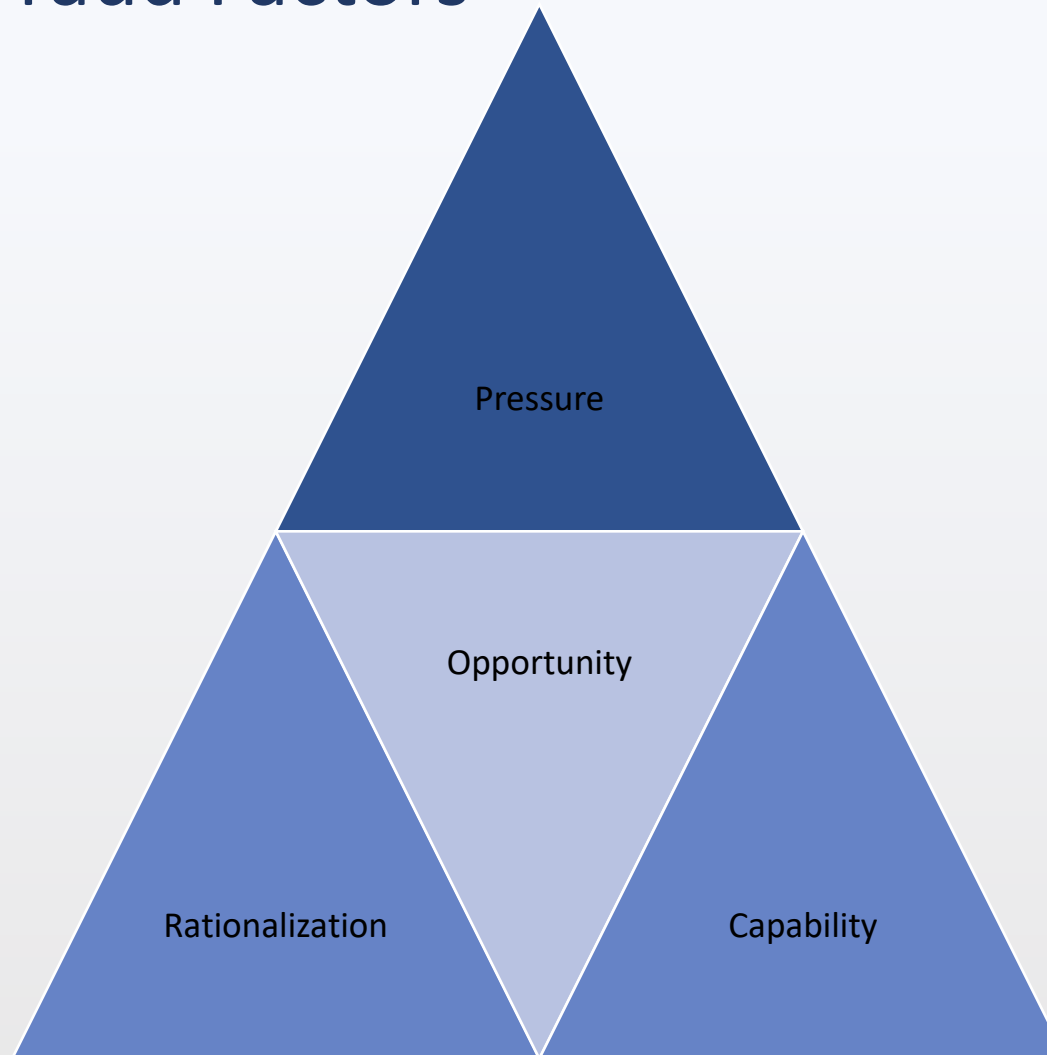
Association of Certified Fraud Examiners, 2020 Report to the Nations₁₂



UNIVERSITY
of ALASKA
Many Traditions One Alaska

Four Fraud Factors

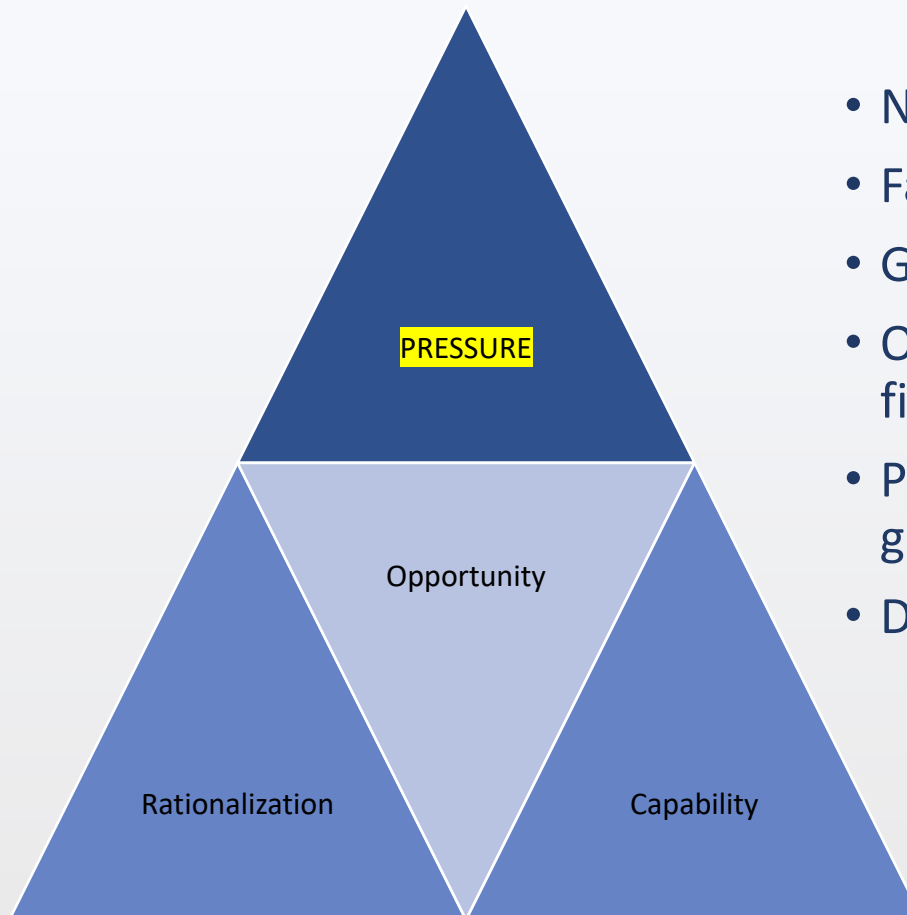
Four Fraud Factors



Published by the ACFE from David T. Wolf and Dana R. Hermanson's paper, "The Fraud Diamond: Considering the Four Elements of Fraud", 2004

14

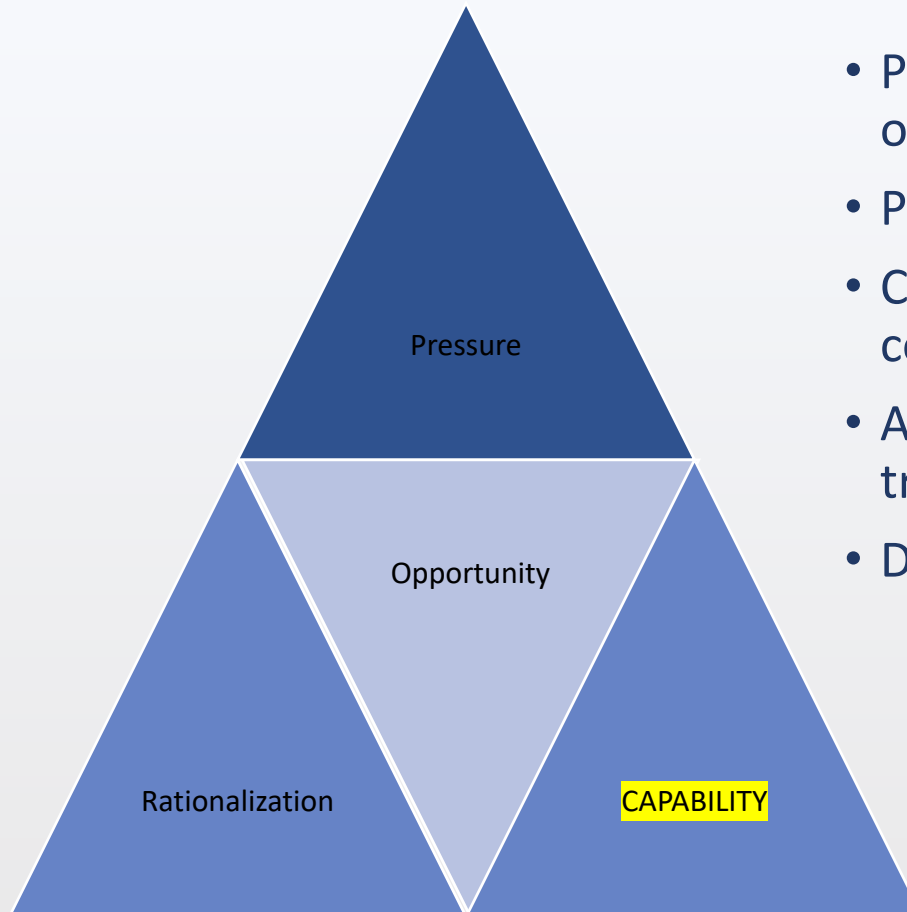
Four Fraud Factors: Pressure



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

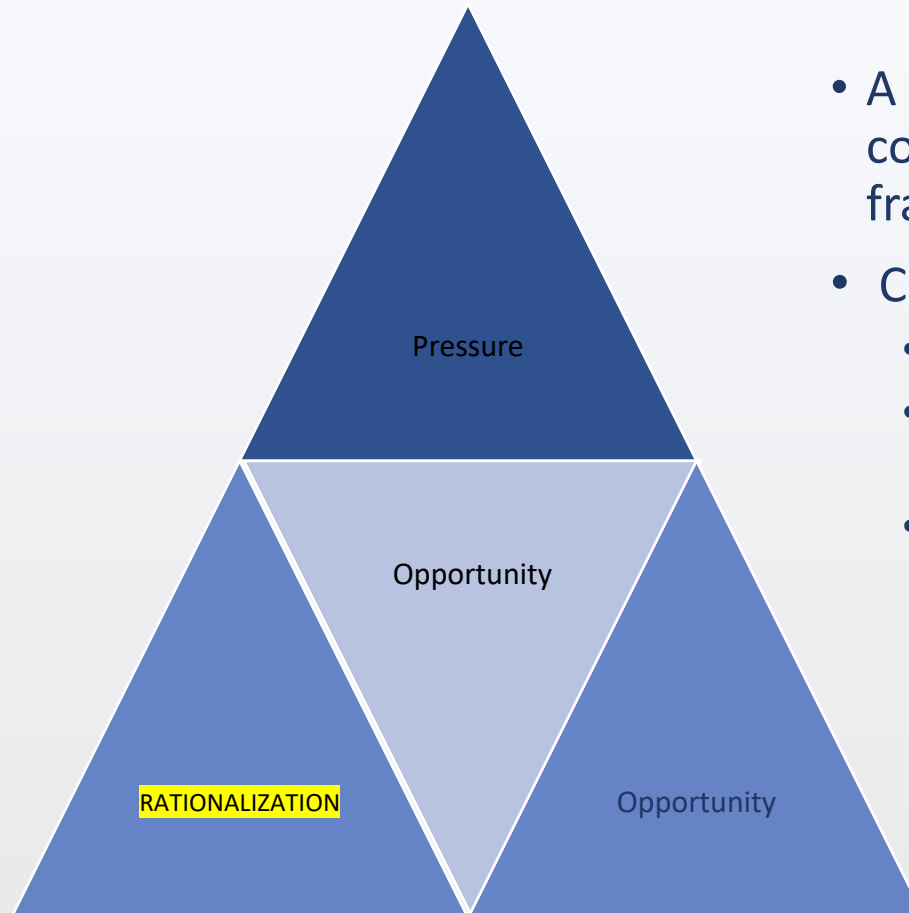
ACFE from Wolfe, David T, and Dana R. Hermanson, *The Fraud Diamond: Considering the Four Elements of Fraud*. (2004)

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.

ACFE from Wolfe, David T, and Dana R. Hermanson, *The Fraud Diamond: Considering the Four Elements of Fraud.* (2004)

Four Fraud Factors: Opportunity

Opportunity to commit fraud arises when employees have access to assets, including information, that allows them to both commit and conceal fraud.

- Weak or non-functioning internal controls
- Poor management supervision, review and approval
- Misuse/abuse of one's position and authority
- Collusion

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

Common Fraud Schemes: High Risk Transaction Areas

- Purchases of Goods and Services
- Cash Receipts
- Payroll
- Procurement Card (Procard)
- Inventory
- Employee Reimbursements
- Personal use of University assets (i.e. computers, vehicles)

Fraud Detection and Prevention

Fraud Detection

Organizations with
FRAUD AWARENESS TRAINING
for employees were
more likely to gather tips through



**FORMAL
REPORTING
MECHANISMS**

56% of tips with training

37% of tips without training



43%

OF SCHEMES WERE DETECTED BY TIP,
and half of those tips
came from employees



TELEPHONE HOTLINE and **EMAIL**
were each used by
whistleblowers in

33%
OF CASES



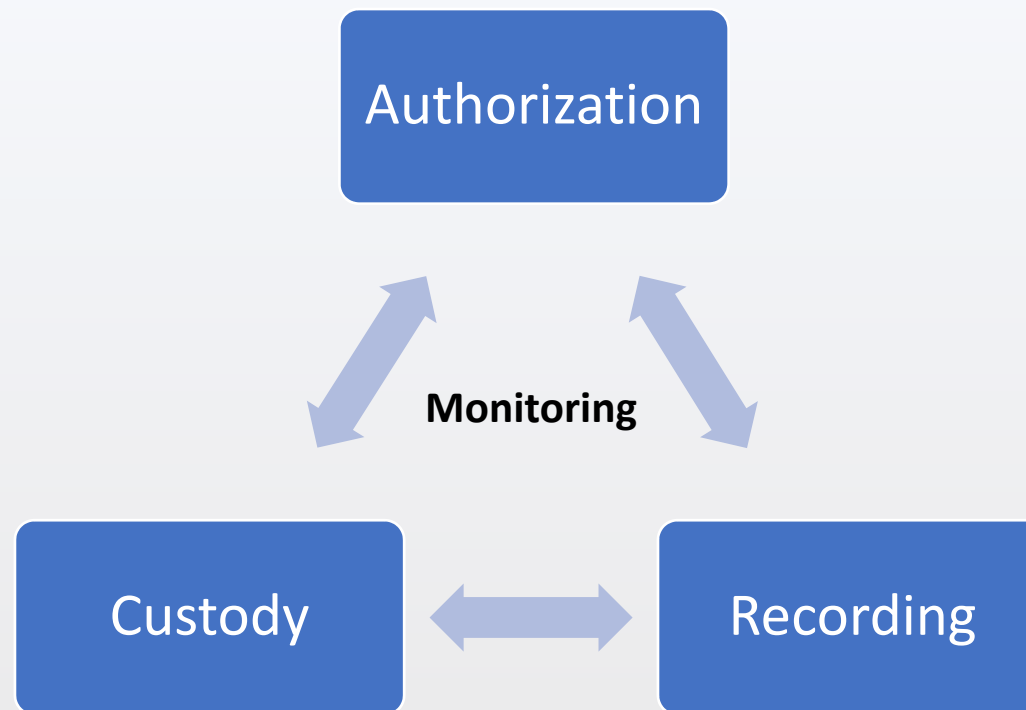
Segregation of Duties

- Is a **preventive control** that is vital in the prevention of fraud and the reduction in or prevention of errors
- Implemented to ensure **no one person** has control over all parts of a transaction
- **Controls** and processes are **designed** to implement a system of checks and balances

Moss Adams, LLP

Segregation of Duties

Functions to be Separated



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

Fraud Cases in the News



Audit finds University of Toledo Employee Embezzlement \$22,000

A fiscal specialist had a UT Federal Credit Union bank account where he was the account holder, although the account was in the university's name.

According to the audit, Woodward diverted over \$30,000 to this account from class fees and donations to the development center he managed at UT. He used almost half of that amount for personal expenses such as credit card payments and insurance bills.

Woodward plead guilty to charges of theft and was ordered to repay the \$22,238 he spent. He resigned his position as fiscal specialist at UT during the audit.



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
- Employee does not take a vacation (years)

Fraud Prevention: Cash Theft

What to monitor:

- Ensure proper Segregation of duties
 - Custody of Assets
 - Check Stock
 - Recording
 - Authorization
 - Detailed reconciliation of monthly ledgers
- Surprise cash counts that agree to supporting documentation
- Refusal to take time off – Highly encourage vacations
- 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 use of the asset
 - Office Space
 - Vehicles
- **Larceny**
 - Purchasing and receiving schemes
 - Asset requisitions and transfers

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
- Conduct regular inventory counts and compare to inventory amounts in tracking system

Asset Misappropriation: Fraudulent Disbursements

Billing schemes

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

Fraud Cases in the News

University of Missouri Employee embezzles \$781,000 to three shell companies



The United States Attorney's Office Western
District of Missouri, 2016

Event: The employee engaged in false invoicing through three shell companies that the employee owned and made personal purchases using a university credit card. He embezzled funds to gamble at area casinos, purchase cars and other luxury items, buy home appliances, remodel a home, take vacations, and pay off bills.

Outcome: The employee was fired after university officials discovered the personal expenses incurred on the procurement credit card. FBI investigated and he was convicted in federal court for embezzling more than \$781,000 over a 13-year period. The court ordered the former employee to pay \$781,000 in restitution and serve a sentence of four years in federal prison.

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

Fraud Cases in the News

Facilities director at
SUNY arrested for
stealing over \$31,999
on school credit card



By Carl Campanile, New York Post, Sept. 18, 2020

Erik Reimann, a former SUNY Empire College facilities director, arrested for 171 unauthorized purchases on a school credit card. These included kitchen appliances, truck and jeep parts, a lawn-mower and snow-blower. Absent supervision and lax internal controls enabled this employee to conceal this misuse of public funds.

Theft was discovered when new Chancellor launched an operational review. The University will be required to reimburse the state for the unauthorized expenditures.

Fraud Prevention: Personal Purchases

Red flags:

- Over purchasing
- Unusually high number of Procard transactions
- Duplicate purchases on Procard on the same approximate date, time, and amount
- Purchasing of items selectively through one vendor

What to monitor:

- Procard Card statements, card sharing, and logs
- UA approvals
 - DO NOT share your UA ID/ 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
 - Over purchasing
- Multiple reimbursements

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
- Does it pass the “sniff” test

Asset Misappropriation: Fraudulent Disbursements

Check tampering schemes:

- Forged maker
- Forged endorsement
- Altered payee

This is easier now with high powered copiers!

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
- Periodically spot check there no missing numbers in check stock

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

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
- FYIs that are setup need to review time records

Corruption: Conflicts of Interest

Types of Conflicts of Interest

- Purchase schemes
- Entitlement schemes
- Conflicts of commitment

Ethics Video from Former General Counsel Mike Hostina

- Relevant examples of Conflicts of Interest in Higher Education
- Long but Worth it!
- https://media.uaf.edu/media/t/0_gs6icdvm

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

Fraud Cases in the News

Ex- director at American
International College
Guilty \$1 million
Kickback Scheme

A former American International College facilities director of facilities plead guilty to nearly \$1 million in bribery scheme from contractors.



By Jeanette DeForge, The Republican, August 31, 2020

“Young steered contracts for construction, repair, maintenance, and other work for the collegiate institutions to favored contractors who paid him bribes, typically in the amount of 15% of the contact.”

Federal Agents approached a contractor who was hired for more than 1.4 million for work on the campus to investigate the kickbacks in 2018. The contractor identified fraudulent invoices he submitted for which no work was completed.

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
- Receiving substandard goods or services

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

Type of information technology scheme where fraudsters trick individuals into divulging information or making unauthorized changes to information.

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: Phishing Schemes

What to monitor:

- Emergency requests for to change account information
 - Vendors
- Requests for Passwords
- Unusual email vernacular
 - Greetings that are not normally used
 - Misspelled words
 - Bad Grammar
 - Sentences or numbers separated by commas instead of periods

When in doubt do not open and do not respond the Phishing email!

Fraud Prevention: What can I do?

Fraud prevention starts with you!

Fraud Prevention: Authorizations, Approvals & Verifications

- Ensure proper segregation of responsibilities
 - No one person should have control of more than one functional process.
Authorization, custody, recording
- Limit authorization authority
 - Ensure only current employees have access
 - Review authorization no less than annually
 - Develop written procedures outlining delegation guidelines
- Secure approvals
 - NEVER sign a blank form
 - Secure access to electronic signatures
- Conduct verifications
 - Compare budgeted with actual expenditures

Fraud Prevention: Review and Verify

Review travel documents, including receipts

- Do not simply sign them electronically and pass them on

Review procurement card statements, including receipts

Do not simply sign them and pass them through

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 employer, but is a routine responsibility in cash handling areas

Fraud Prevention: Secure Passwords and Email

No Password Sharing

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

Fraud Prevention: Ask Questions & Conduct Training

Ask Questions

- Professional skepticism
- Make time for staff training
- Company policies and procedures
- Report it to your supervisor, University Police, or General Counsel
- Contact the Office of Audit and Consulting Services by phone or email
 - Phone – 907-786-7756 or 907-450-8094
 - Email – nrcountryman@alaska.edu or nlpittman@alaska.edu
- Report your suspicions anonymously at:
 - www.alaska.ethicspoint.com

UA Confidential Hotline

Hosted by NAVEX Global “EthicsPoint”

- EthicsPoint is used by hundreds of higher education institutions
- Third-party hosted to provide the best option for anonymity
- Available via
 - web intake www.alaska.ethicspoint.com
 - toll-free telephone (855-251-5719)
- Different types of issues/concerns can be reported:
 - Financial: fraud, waste, abuse
 - Ethical misconduct
 - Safety and environmental
 - Compliance
 - Human resources (i.e.: bullying)
 - Protection of minors



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.
- The Fraud Diamond: Considering the Four Elements of Fraud. David T. Wolfe and Dana R. Hermanson. 2004
- 2019 Fraud Examiner's Manual, ACFE, 2019.
- System Office of Audit and Consulting Services Website
 - A&CS Internal Controls
 - Self-Assessment Questionnaires

University of Alaska System Office of Audit and Consulting Services

For more information, contact

Niki Countryman, CPA, CIA, CMA, CFE

Senior Internal Auditor

(907)786-7756

nrcountryman@alaska.edu or

A&CS Department email: ua-ia-dept@alaska.edu

For additional training resources and presentation slides, see

System Office of Audit and Consulting Services

<http://www.alaska.edu/audit/>

Fraud Prevention

It Starts with You!