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 Compliance Services
December 2023

UNIVERSITY *of* ALASKA
Many Traditions One Alaska

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

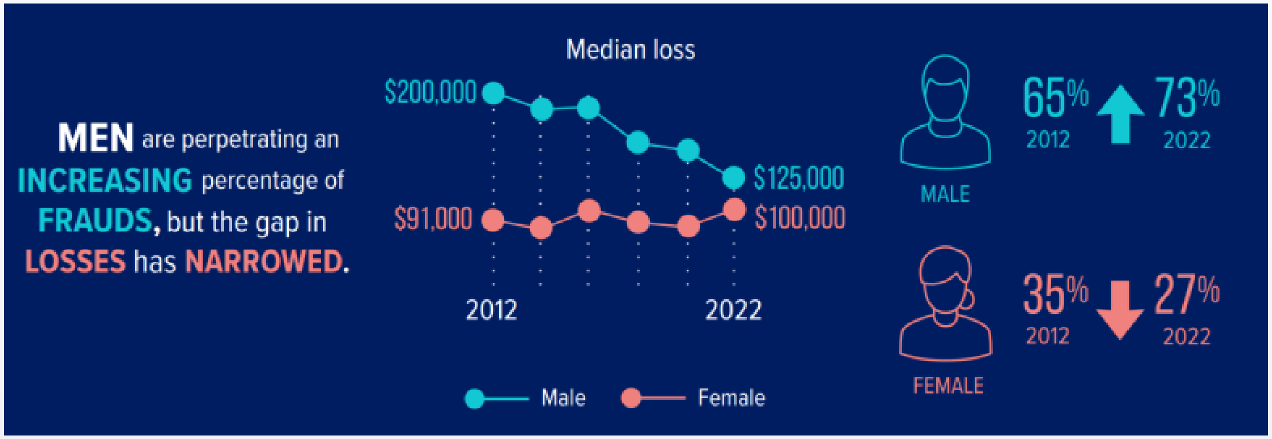
The Institute of Internal Auditors

Learning Objectives

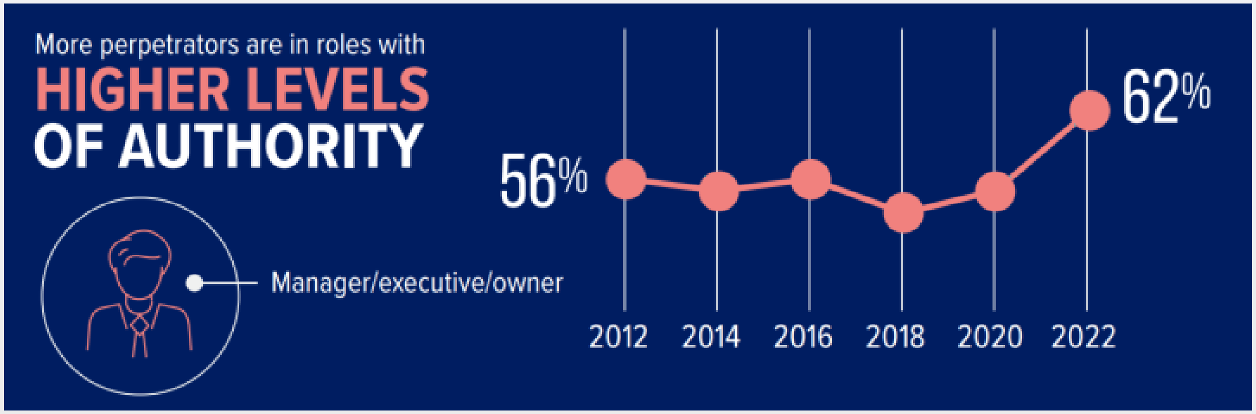
- Explore Red Flags
  - Behavioral Facts
  - How Fraudsters Conceal their Fraud
- Identify Ways to Prevent and Detect Fraud
- Fraud Scenarios
- Prevention and Detection controls
  - What can you do if fraud is suspected?
- Resources

Identify the Fraudster

Profile of a Fraudster

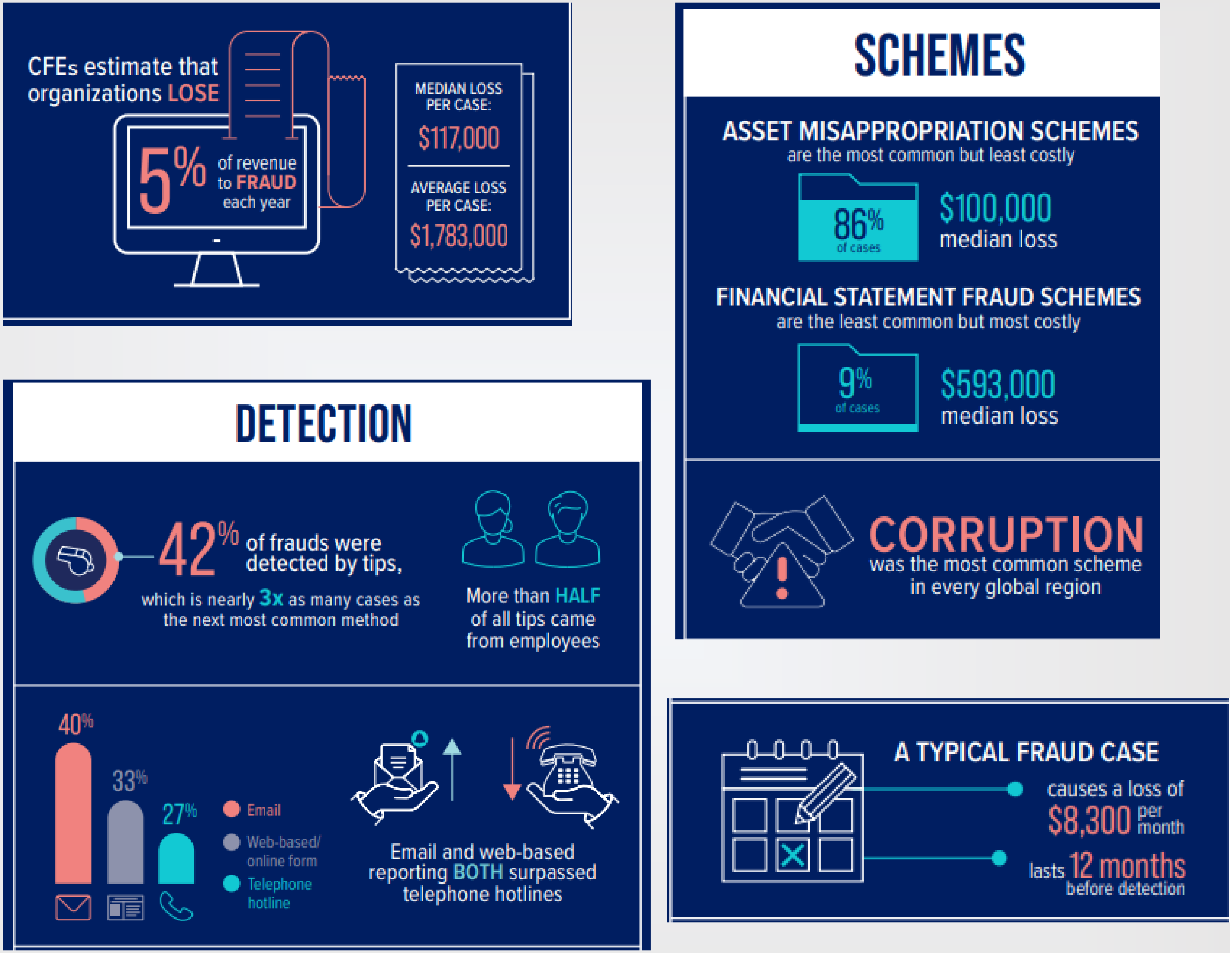


MEN are perpetrating an **INCREASING** percentage of **FRAUDS,** but the gap in **LOSSES** has **NARROWED.**



More perpetrators are in roles with **HIGHER LEVELS OF AUTHORITY**

Association of Certified Fraud Examiners 2022 Report to the Nations



CFEs estimate that organizations LOSE 5% of revenue to FRAUD each year

MEDIAN LOSS PER CASE: $117,000

AVERAGE LOSS PER CASE: $1,783,000

DETECTION

42% of frauds were detected by tips, which is nearly 3x as many cases as the next most common method

More than HALF of all tips came from employees

40%
33%
27%
● Email
● Web-based/ online form
● Telephone hotline

Email and web-based reporting BOTH surpassed telephone hotlines

SCHEMES

ASSET MISAPPROPRIATION SCHEMES

are the most common but least costly

86% of cases

$100,000 median loss

FINANCIAL STATEMENT FRAUD SCHEMES

are the least common but most costly

9% of cases

$593,000 median loss

CORRUPTION was the most common scheme in every global region

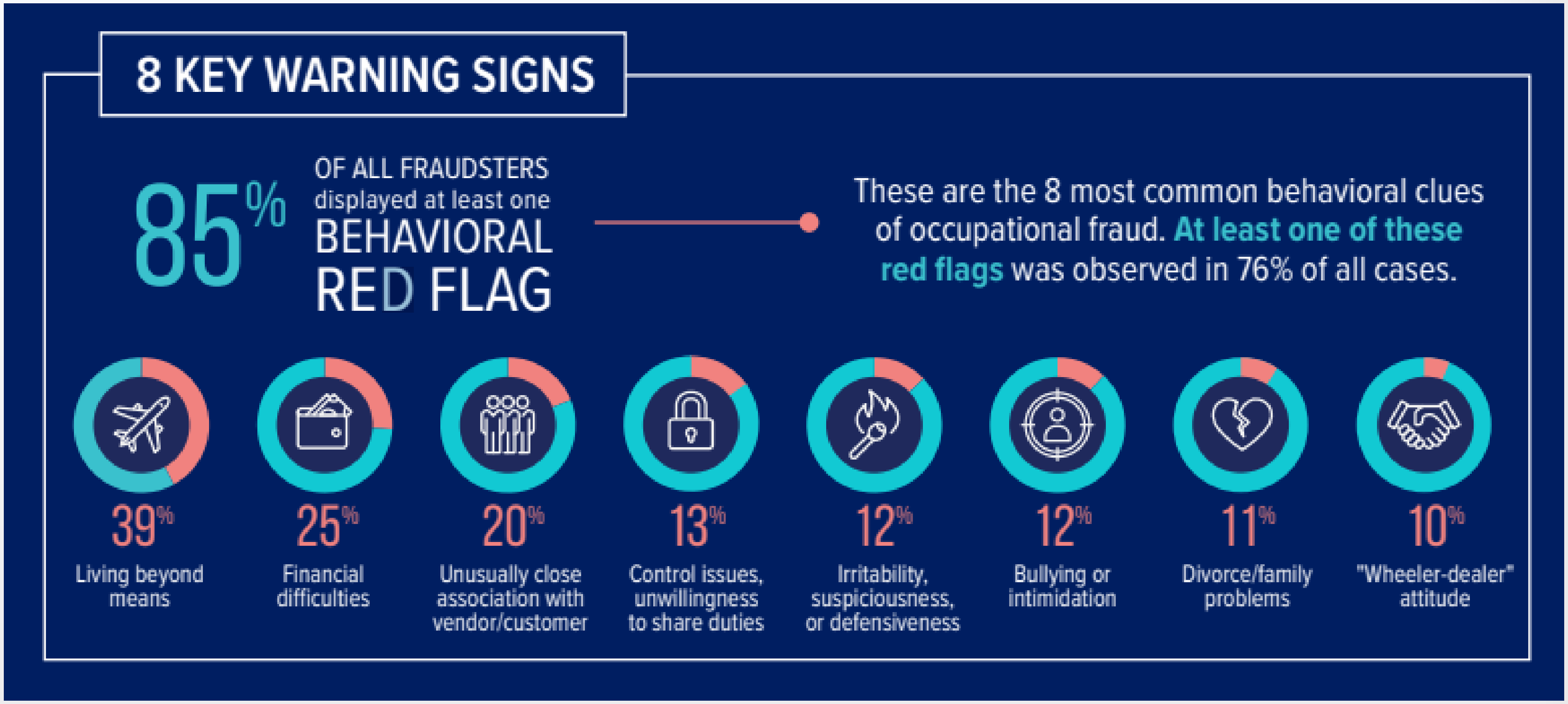
A TYPICAL FRAUD CASE

causes a loss of $8,300 per month

lasts 12 months before detection

Association of Certified Fraud Examiners 2022 Report to the Nations

Behavioral Red Flags of Fraud



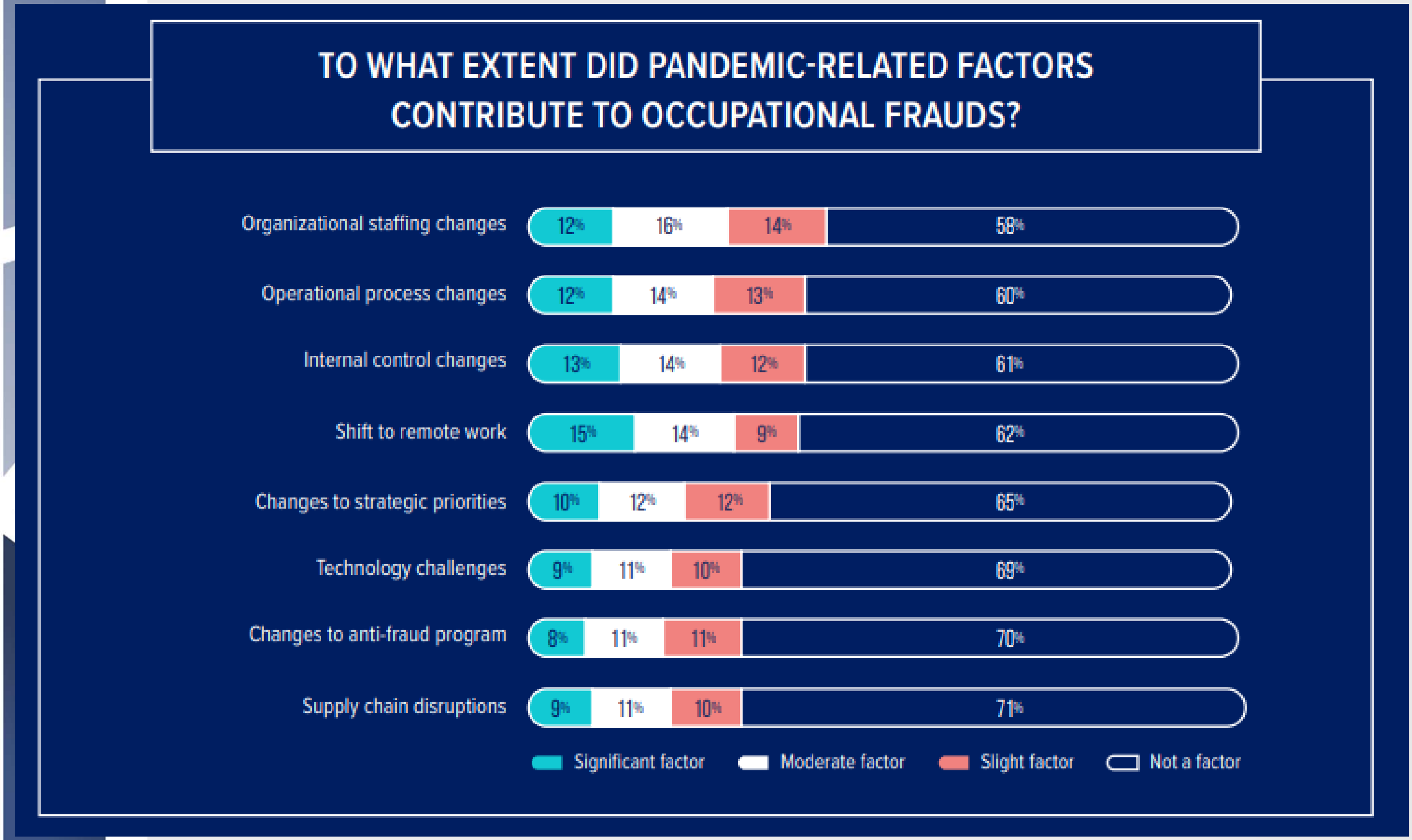
8 KEY WARNING SIGNS

85% OF ALL FRAUDSTERS displayed at least one BEHAVIORAL RED FLAG

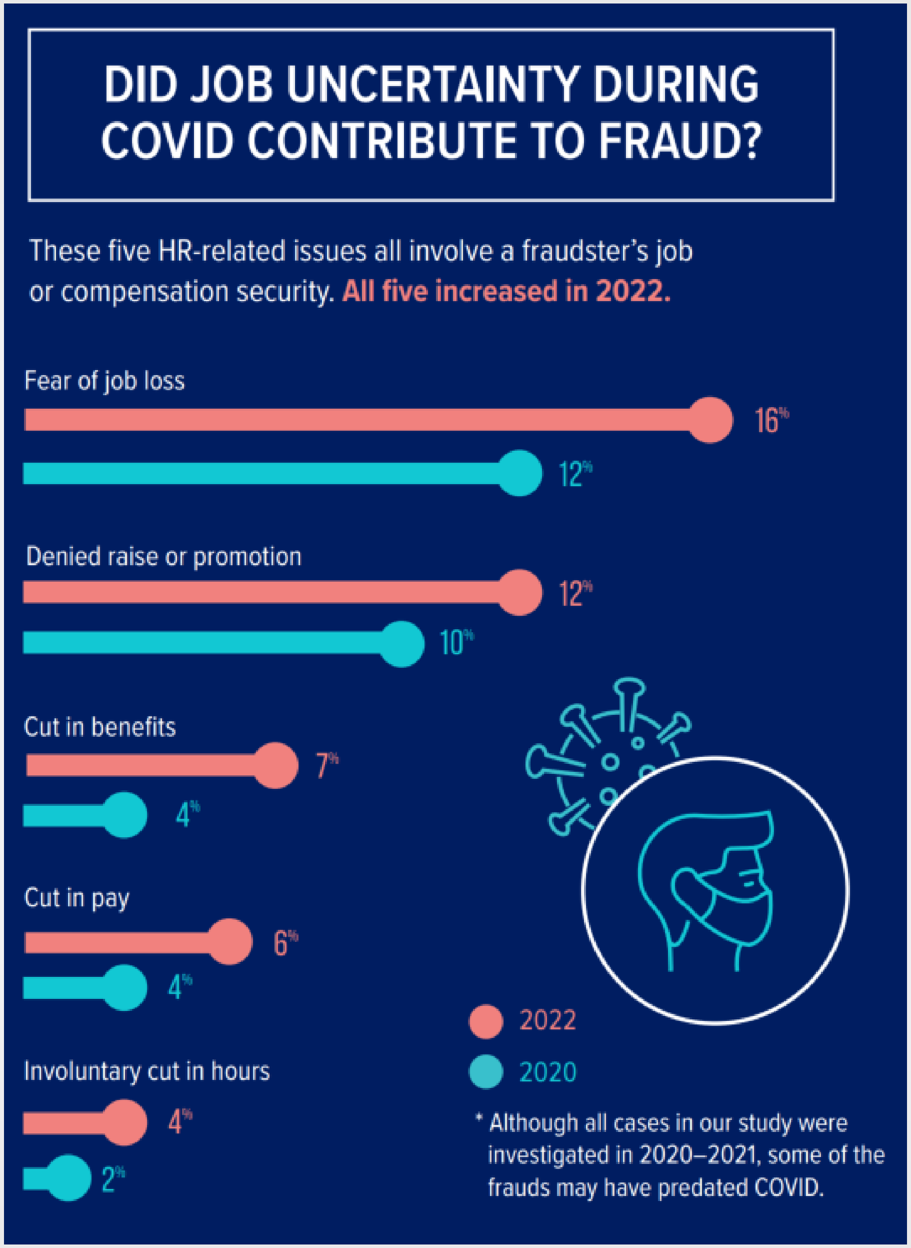
These are the 8 most common behavioral clues of occupational fraud. **At least one of these red flags** was observed in 76% of all cases.

- 39% Living beyond means
- 25% Financial difficulties
- 20% Unusually close association with vendor/customer
- 13% Control issues, unwillingness to share duties
- 12% Irritability, suspiciousness, or defensiveness
- 12% Bullying or intimidation
- 11% Divorce/family problems
- 10% "Wheeler-dealer" attitude

Association of Certified Fraud Examiners, 2022 Report to the Nations



Association of Certified Fraud Examiners, 2022 Report to the Nations



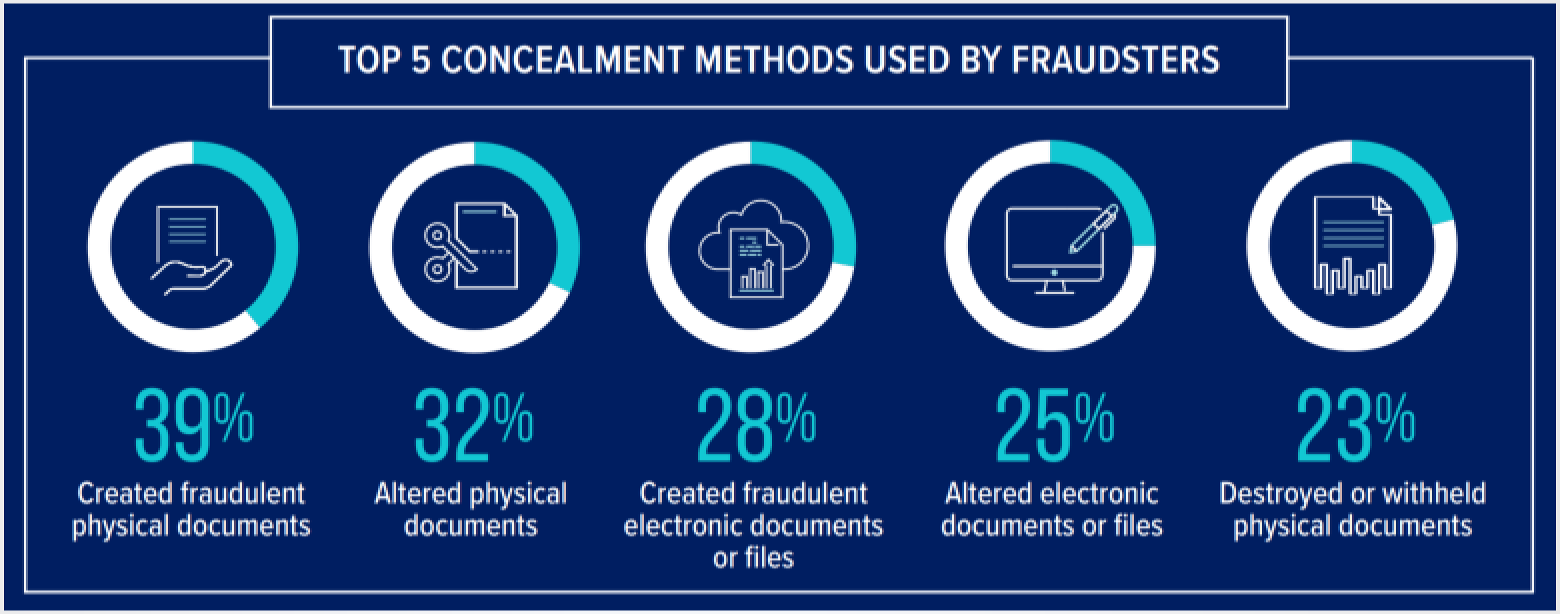
DID JOB UNCERTAINTY DURING COVID CONTRIBUTE TO FRAUD?

These five HR-related issues all involve a fraudster's job or compensation security. **All five increased in 2022.**

* Although all cases in our study were investigated in 2020–2021, some of the frauds may have predated COVID.

Association of Certified Fraud Examiners, 2022 Report to the Nations

Fraud Methods



TOP 5 CONCEALMENT METHODS USED BY FRAUDSTERS

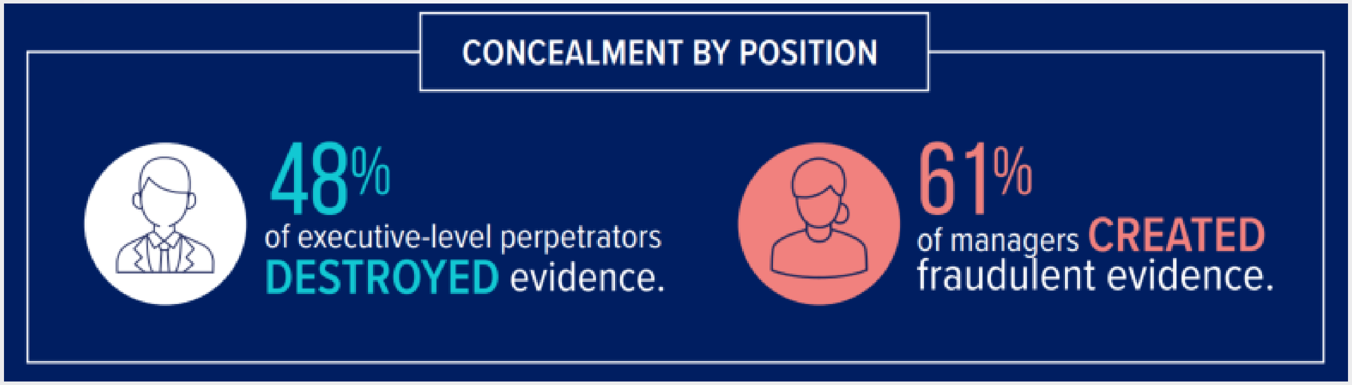
39% Created fraudulent physical documents

32% Altered physical documents

28% Created fraudulent electronic documents or files

25% Altered electronic documents or files

23% Destroyed or withheld physical documents



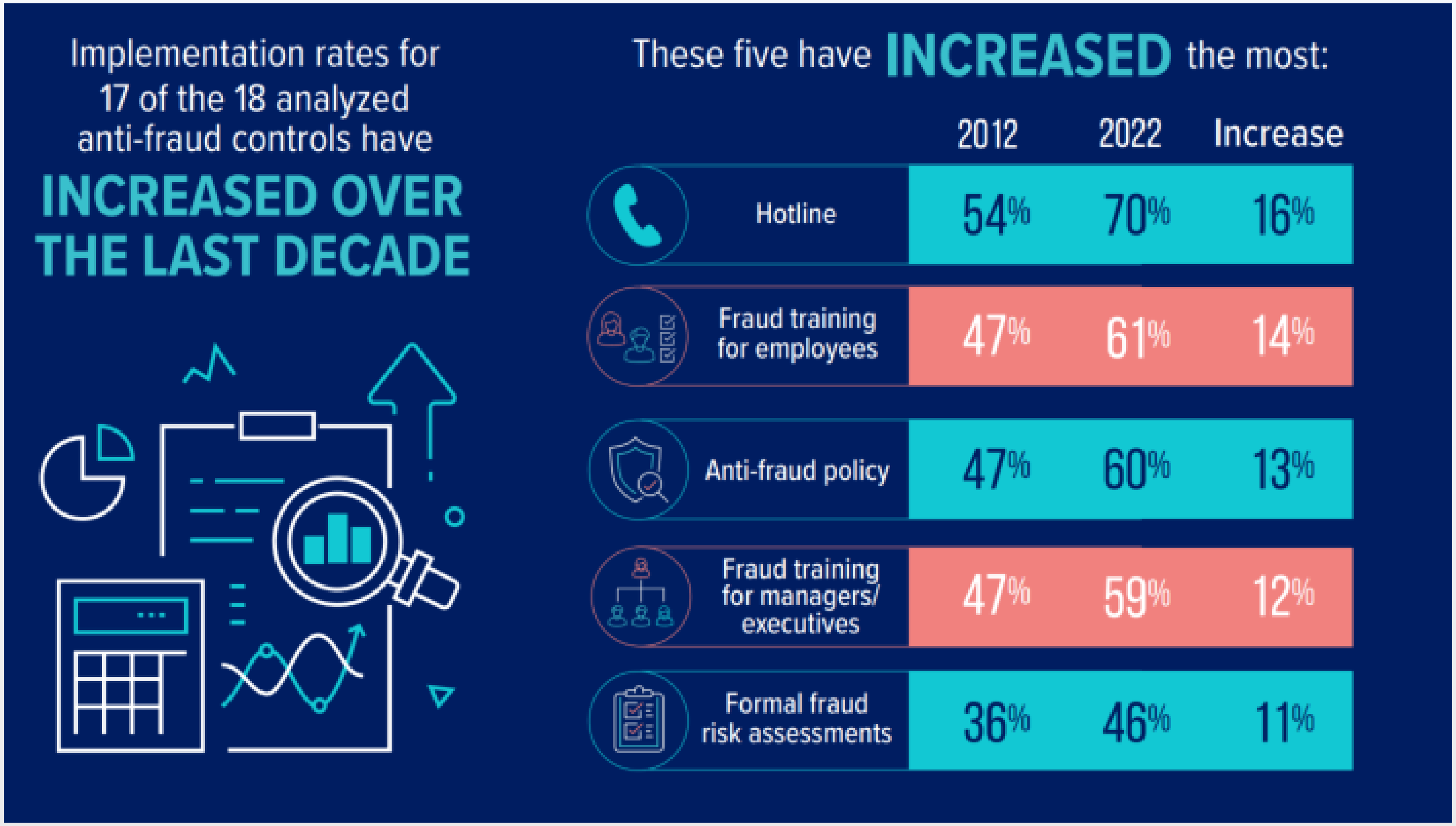
CONCEALMENT BY POSITION

48% of executive-level perpetrators DESTROYED evidence.

61% of managers CREATED fraudulent evidence.

Association of Certified Fraud Examiners, 2022 Report to the Nations

Fraud Controls



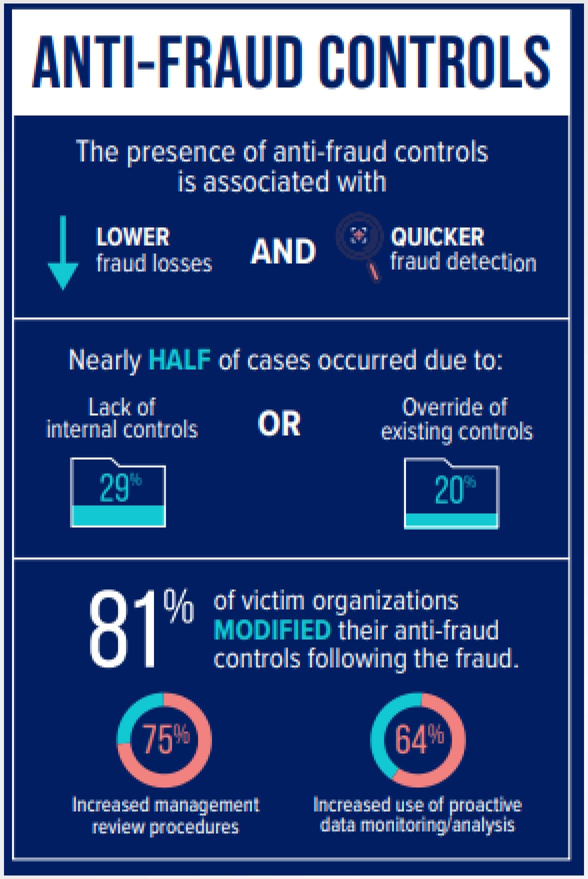
Implementation rates for 17 of the 18 analyzed anti-fraud controls have

INCREASED OVER THE LAST DECADE

These five have **INCREASED** the most:

	2012	2022	Increase
Hotline	54%	70%	16%
Fraud training for employees	47%	61%	14%
Anti-fraud policy	47%	60%	13%
Fraud training for managers/ executives	47%	59%	12%
Formal fraud risk assessments	36%	46%	11%

Association of Certified Fraud Examiners, 2022 Report to the Nations



ANTI-FRAUD CONTROLS

The presence of anti-fraud controls is associated with

LOWER fraud losses AND QUICKER fraud detection

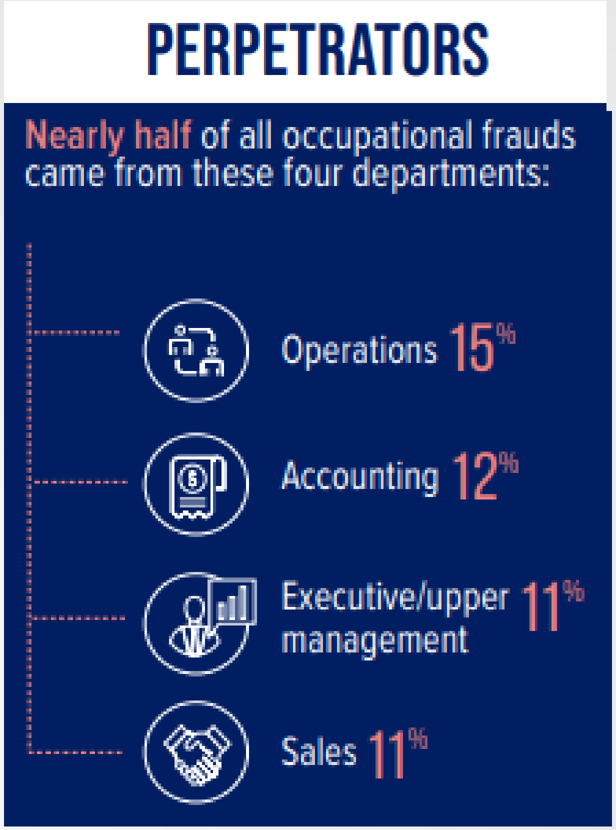
Nearly HALF of cases occurred due to:

Lack of internal controls 29% OR Override of existing controls 20%

81% of victim organizations MODIFIED their anti-fraud controls following the fraud.

75% Increased management review procedures

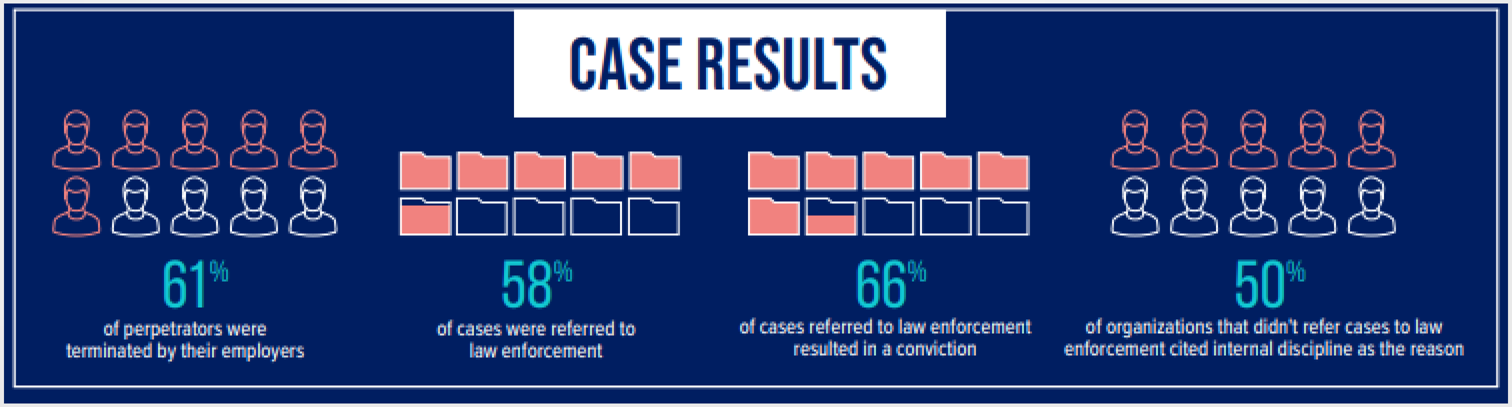
64% Increased use of proactive data monitoring/analysis



PERPETRATORS

Nearly half of all occupational frauds came from these four departments:

Operations	15%
Accounting	12%
Executive/upper management	11%
Sales	11%



CASE RESULTS

61% of perpetrators were terminated by their employers

58% of cases were referred to law enforcement

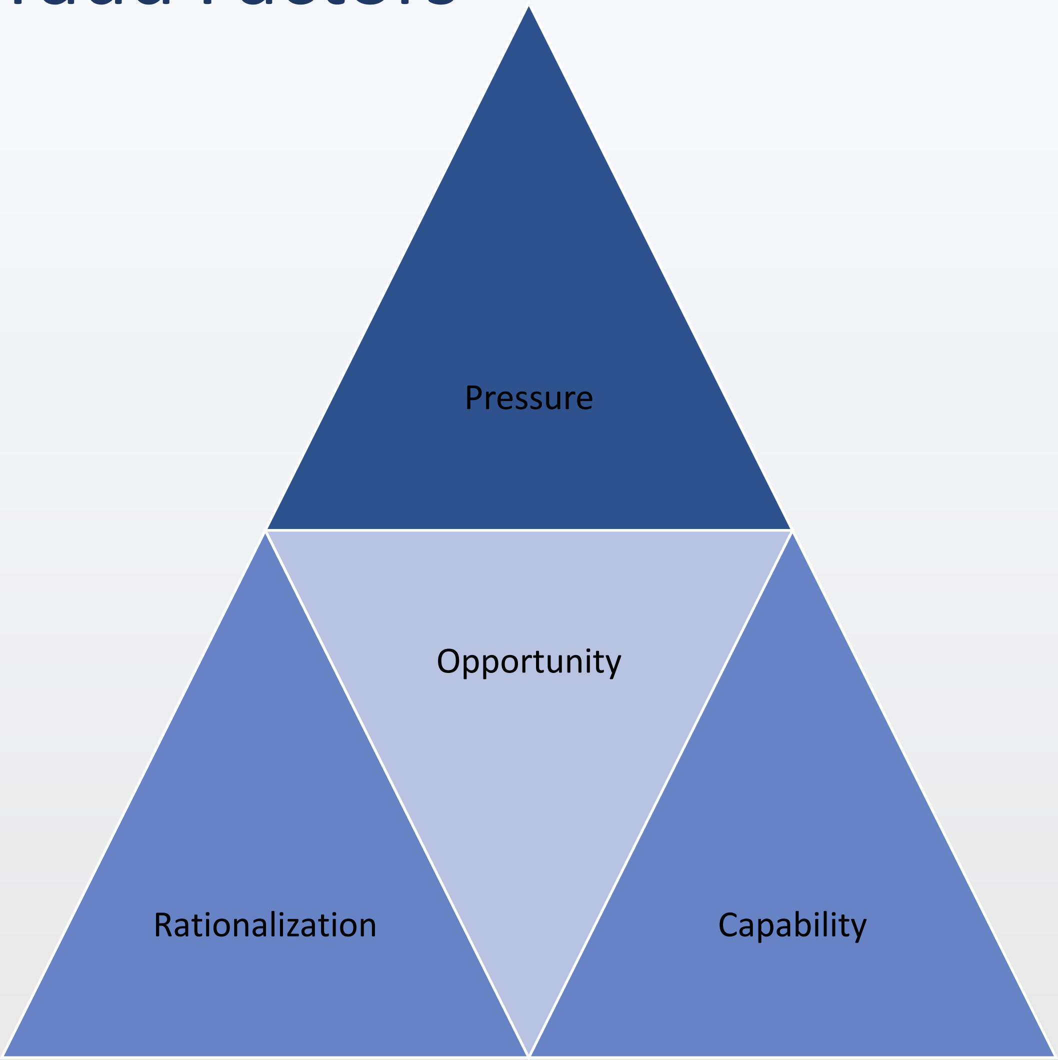
66% of cases referred to law enforcement resulted in a conviction

50% of organizations that didn't refer cases to law enforcement cited internal discipline as the reason

Association of Certified Fraud Examiners, 2022 Report to the Nations

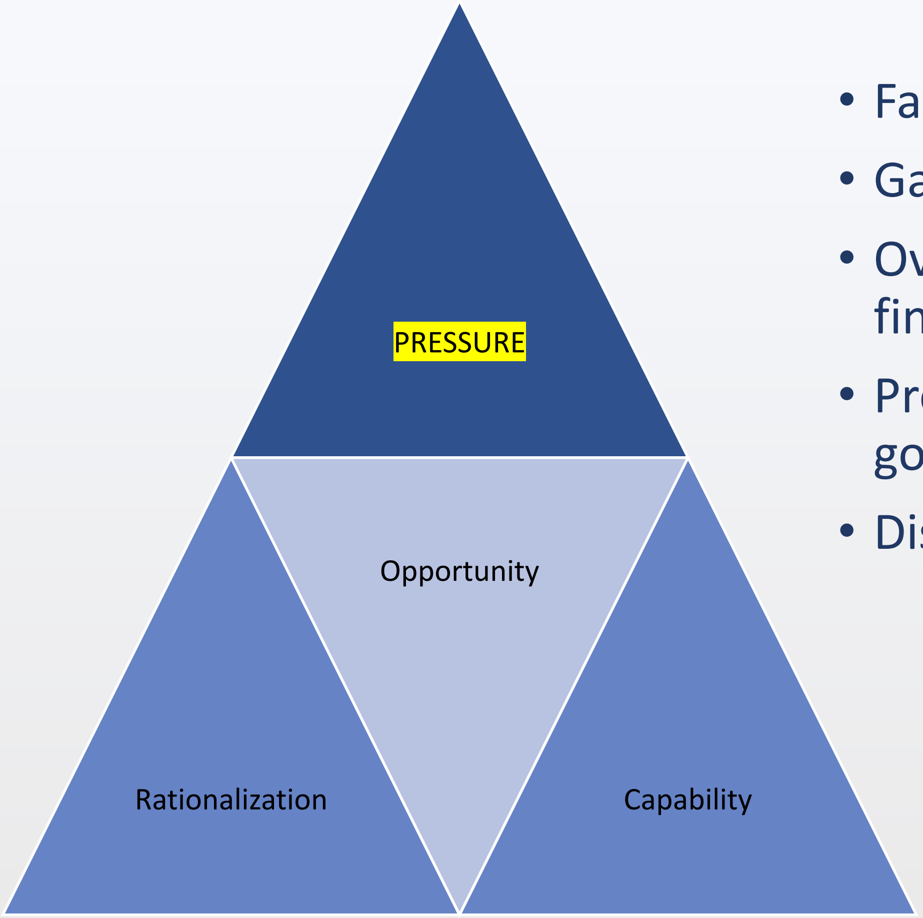
Factors Contributing to Fraud

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

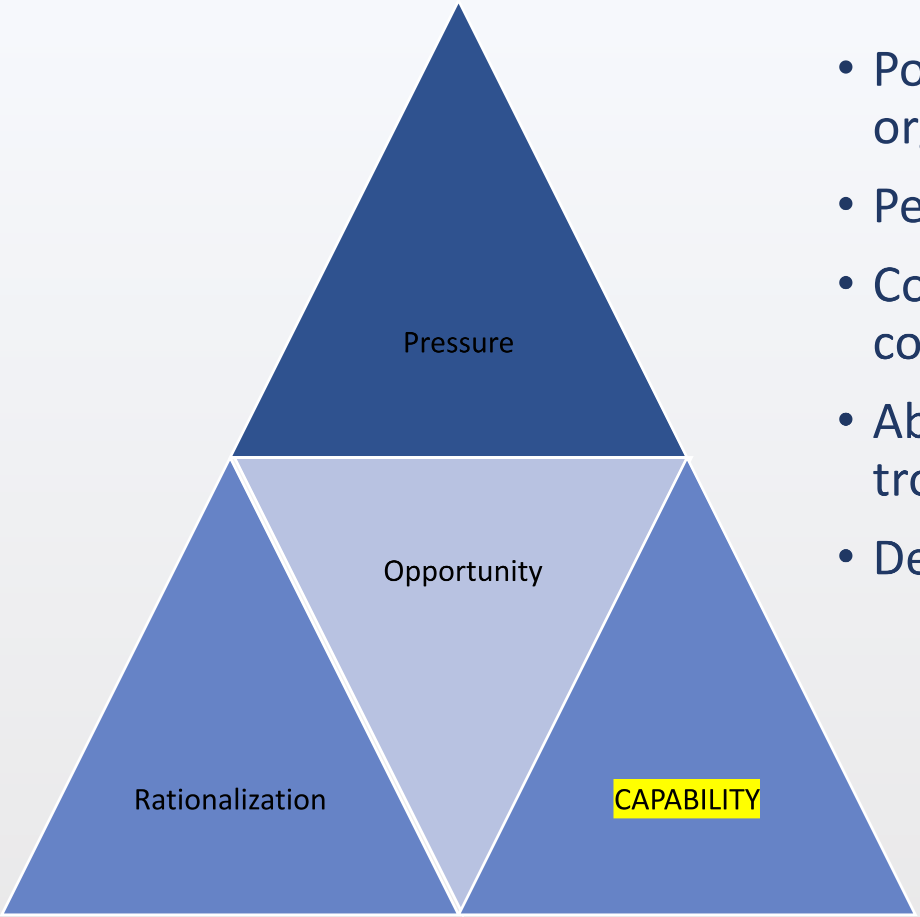
Four Fraud Factors: Pressure



- 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)

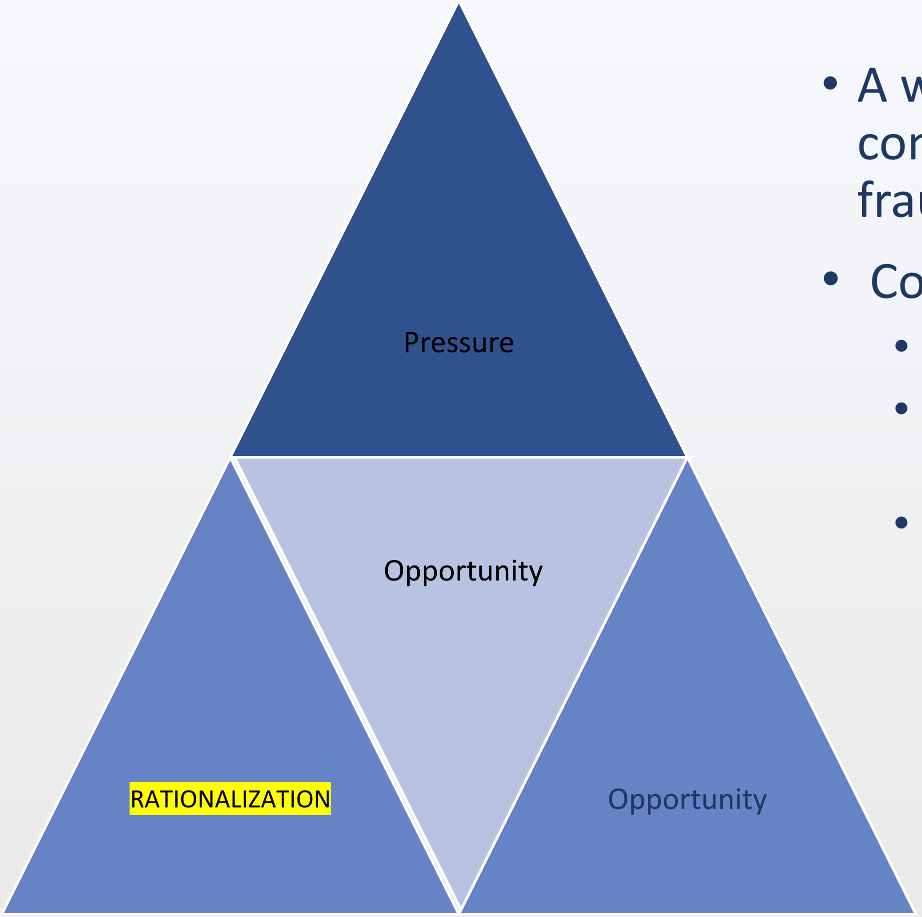
Four Fraud Factors: Capability



- 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

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

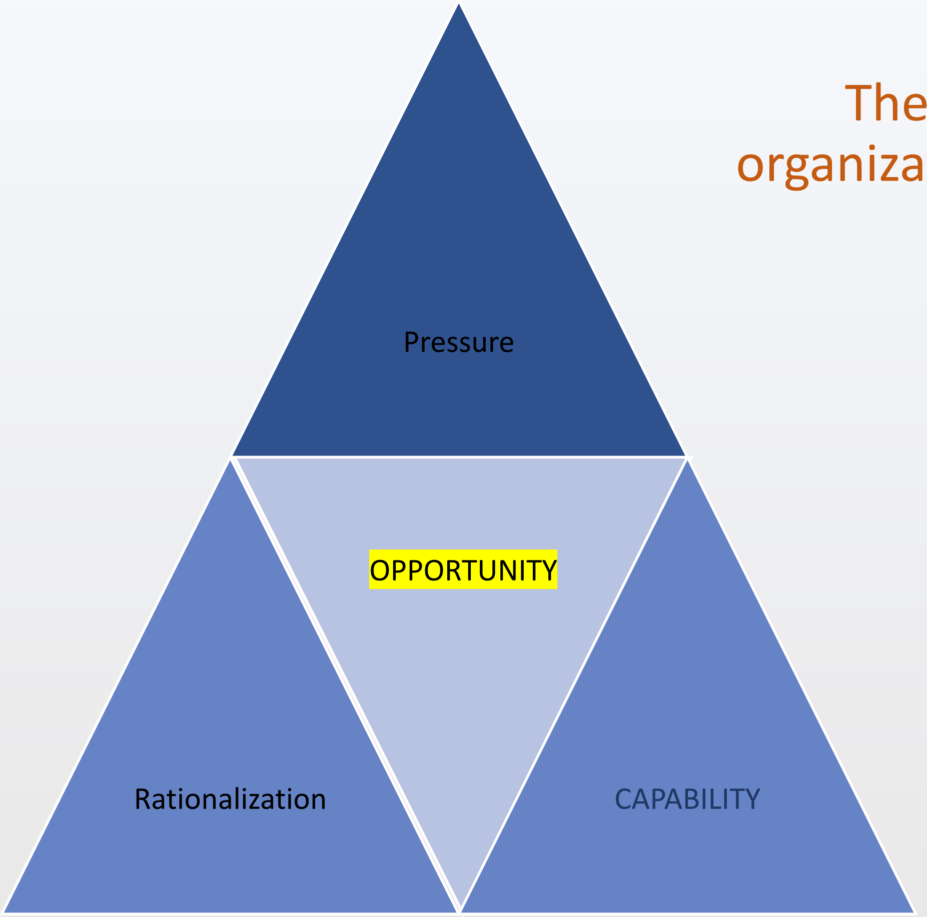
Four Fraud Factors: Rationalization



- 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

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

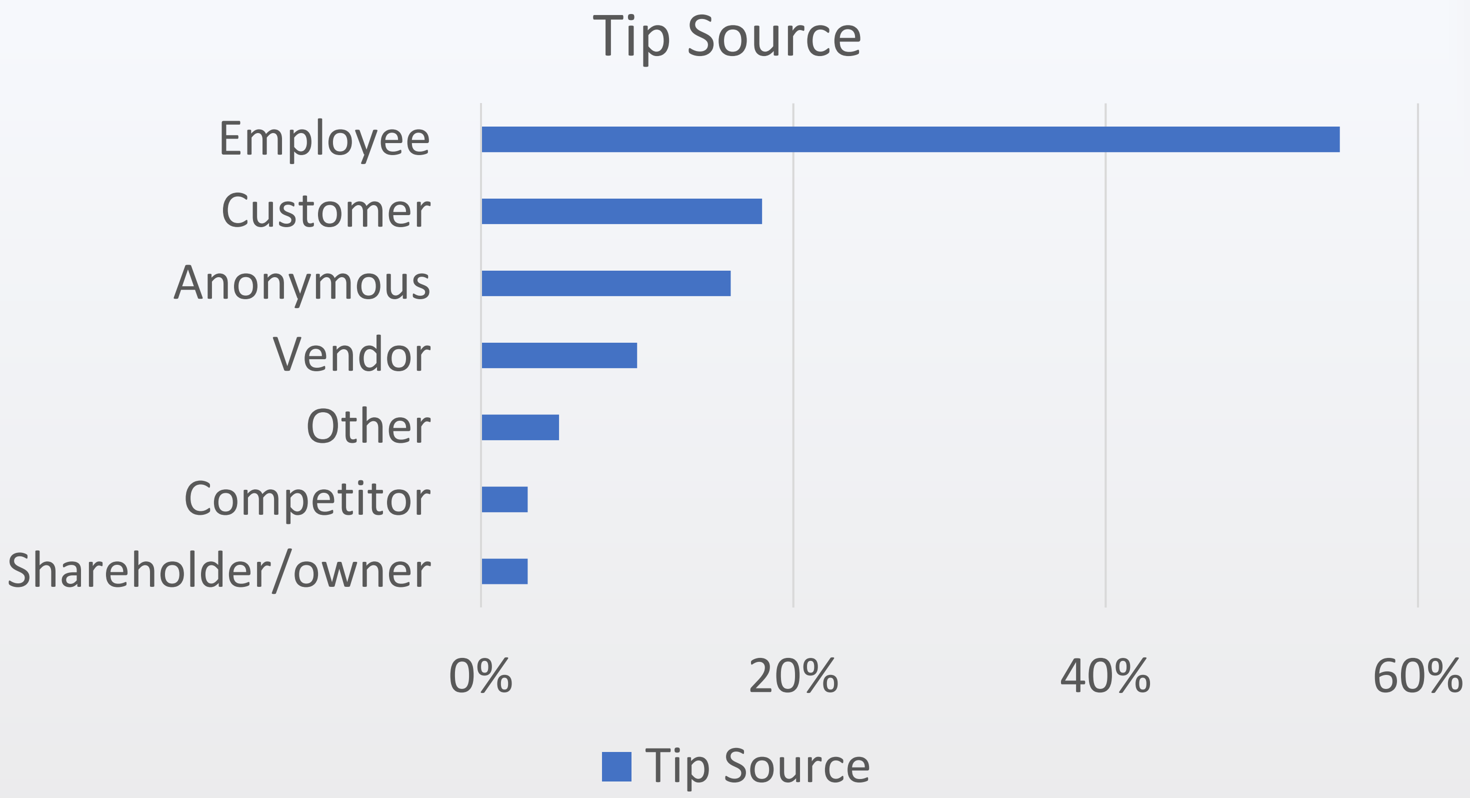
Four Fraud Factors: Opportunity



The only aspect the organization really controls is opportunity.

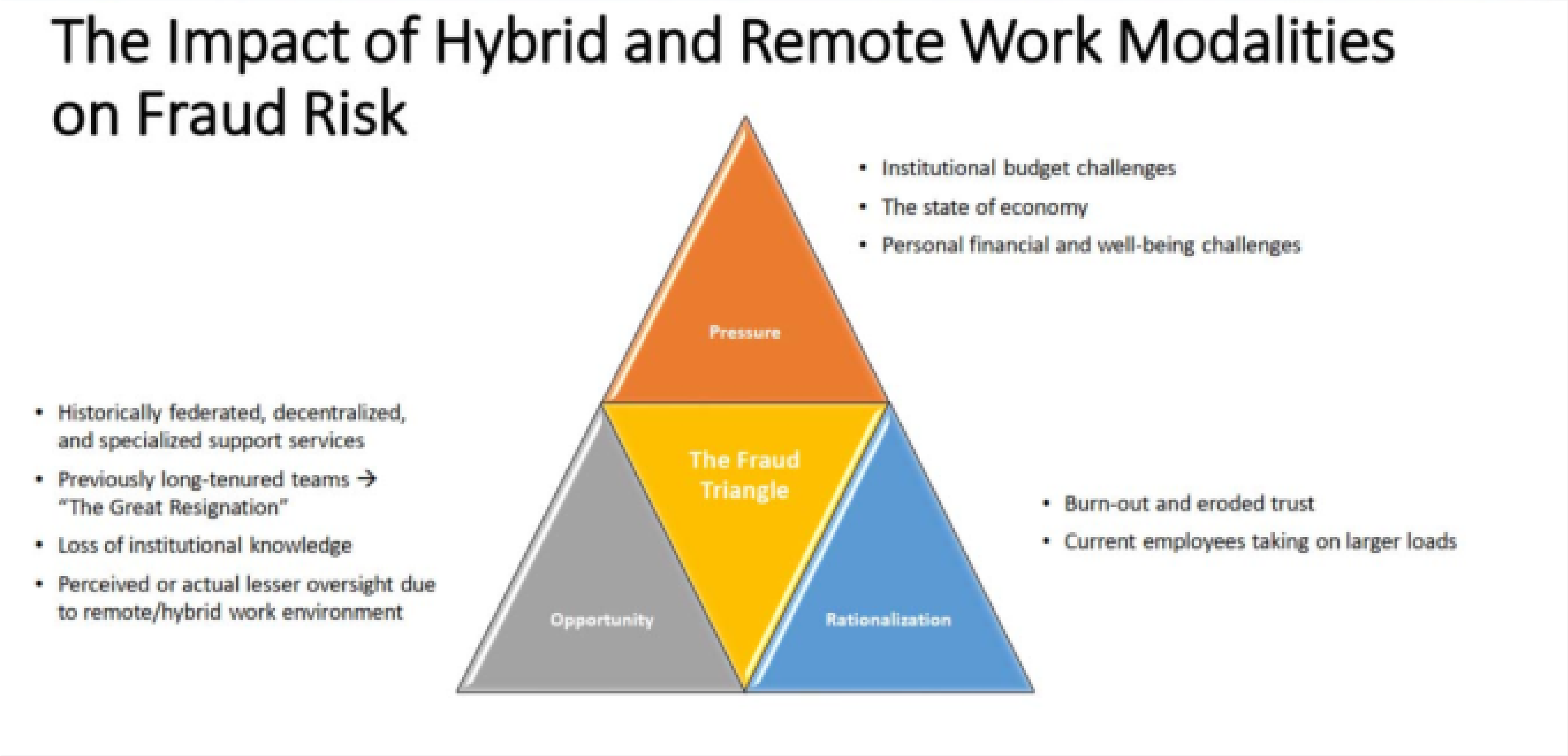
ACFE from Wolfe, David T, and Dana R. Hermanson,
The Fraud Diamond: Considering the Four Elements of Fraud. (2004)

Fraud Facts



Association of Certified Fraud Examiners
2022 Report to the Nations

Four Fraud Factors



The Impact of Hybrid and Remote Work Modalities on Fraud Risk

The Fraud Triangle

Pressure

- Institutional budget challenges
- The state of economy
- Personal financial and well-being challenges

Opportunity

- Historically federated, decentralized, and specialized support services
- Previously long-tenured teams → "The Great Resignation"
- Loss of institutional knowledge
- Perceived or actual lesser oversight due to remote/hybrid work environment

Rationalization

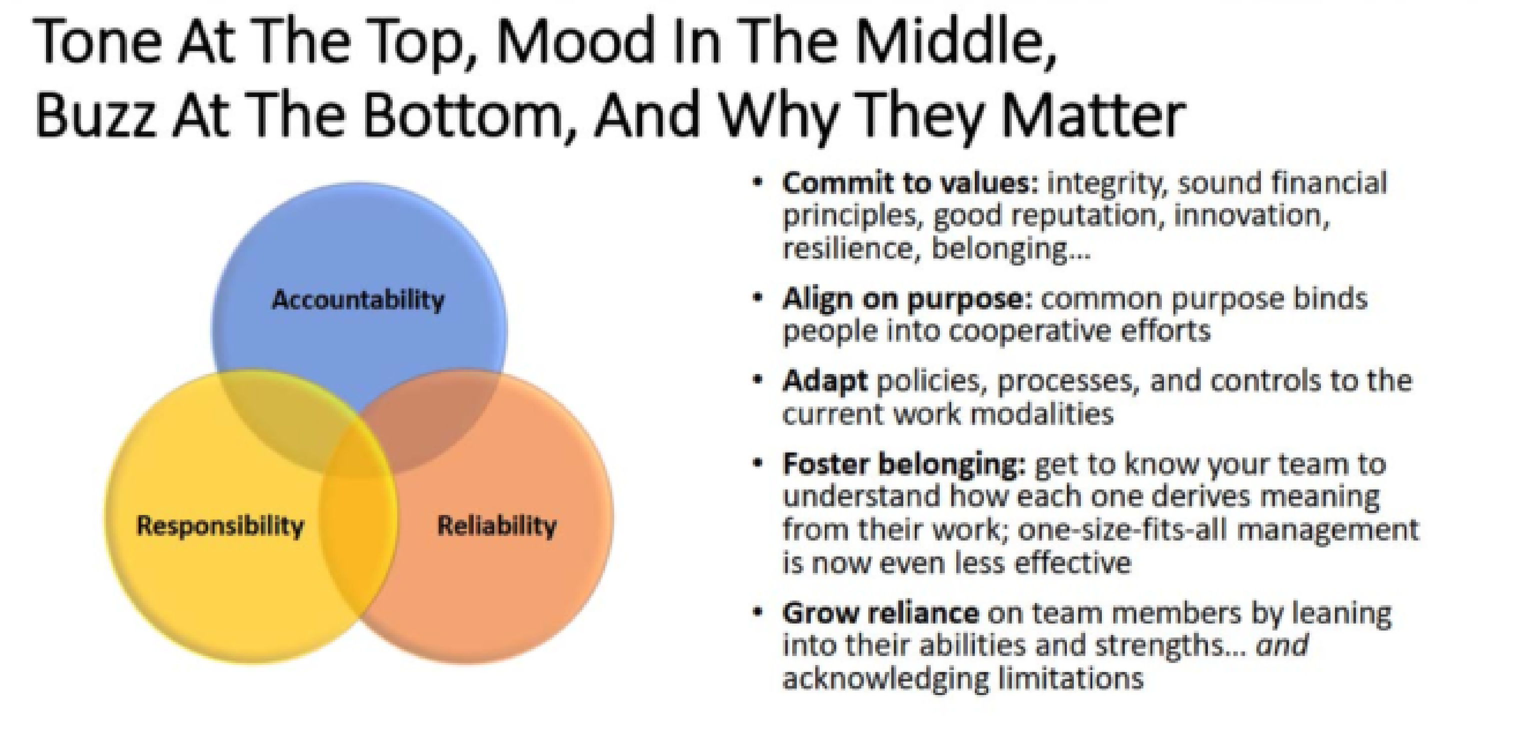
- Burn-out and eroded trust
- Current employees taking on larger loads

Four Fraud Factors: Opportunity

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

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

Organizational Culture



Tone At The Top, Mood In The Middle, Buzz At The Bottom, And Why They Matter

Accountability
Responsibility
Reliability

- **Commit to values:** integrity, sound financial principles, good reputation, innovation, resilience, belonging…
- **Align on purpose:** common purpose binds people into cooperative efforts
- **Adapt** policies, processes, and controls to the current work modalities
- **Foster belonging:** get to know your team to understand how each one derives meaning from their work; one-size-fits-all management is now even less effective
- **Grow reliance** on team members by leaning into their abilities and strengths… *and* acknowledging limitations

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

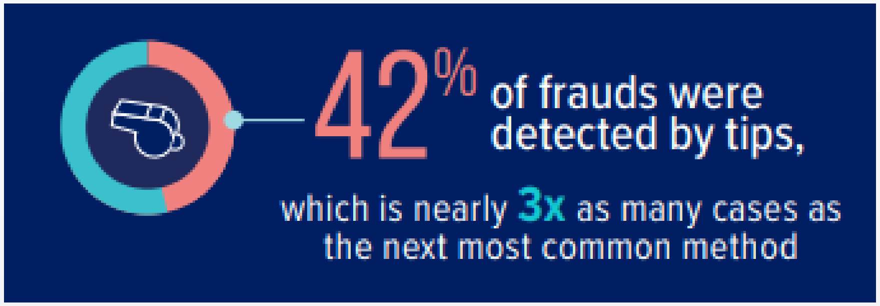
- Conflicts of Interest
- Bribery and Incentives
- Information Technology

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, research labs and equipment)

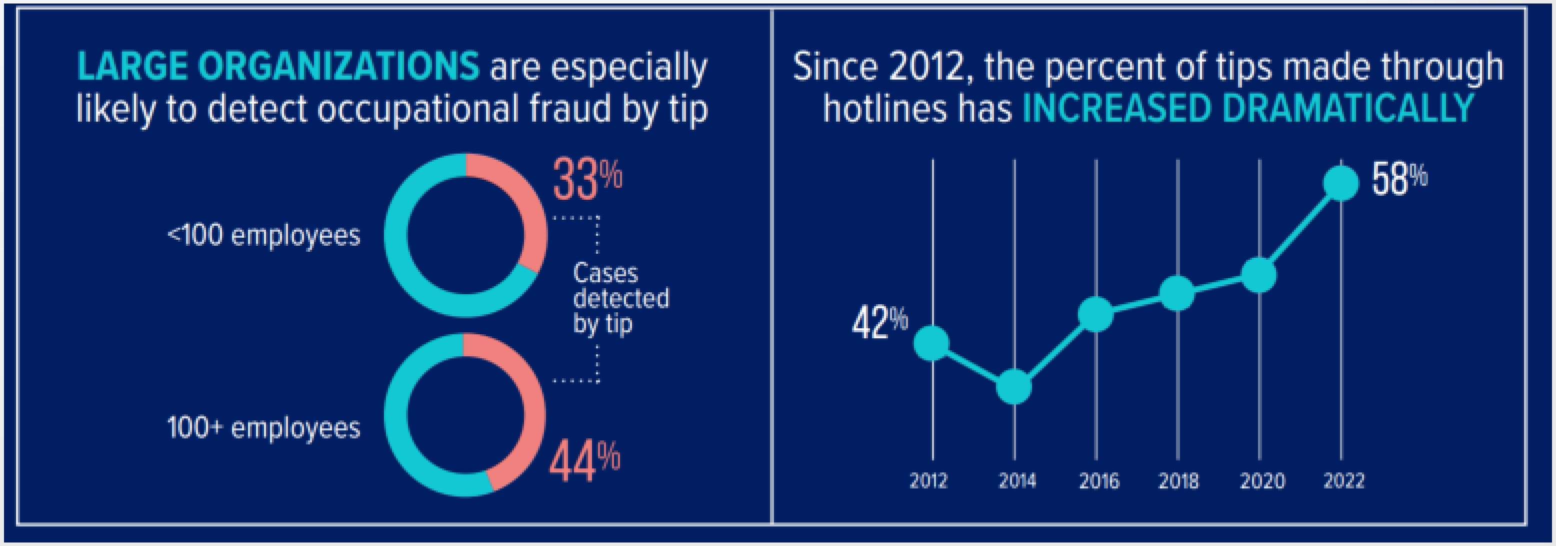
Fraud Detection and Prevention

Fraud Detection



42% of frauds were detected by tips,

which is nearly 3x as many cases as the next most common method



LARGE ORGANIZATIONS are especially likely to detect occupational fraud by tip

Since 2012, the percent of tips made through hotlines has INCREASED DRAMATICALLY

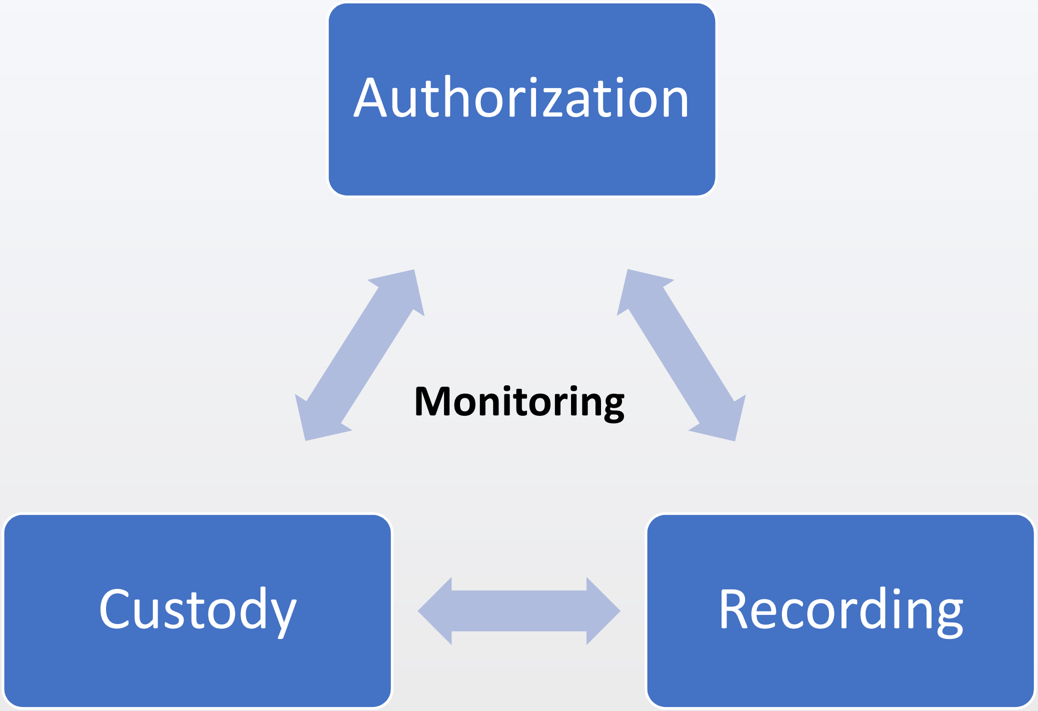
Association of Certified Fraud Examiners, 2022 Report to the Nations

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
  - Frequently rotate duties (cross-train)
  - Monitor password use and attendance

Segregation of Duties

Functions to be Separated



Authorization

Monitoring

Custody

Recording

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

Indiana University

Audit finds Indiana University Foundation Embezzlement of over $300,000

Foundation employee committed wire fraud by stealing $326,334 in charitable donations. Worked as a deposit and payroll deduction associate from 1988 to 2019. Job duties required her to handle money directly, including being the only employee in charge of recording cash donations.

How she did it:

- Stole the days checks and did not record in finance software
- Replaced with next days checks
- Wrote checks from her own personal bank

How it was discovered:

- Foundation discovered accounting irregularities
- Conducted an external audit

Outcome:

- Plead guilty and sentenced to a year and a day in prison
- Ordered to pay $326,334 in restitution

By Emma Flynn, Indiana Daily Student, Nov. 9, 2023

Asset Misappropriation: Cash

Lapping: Stolen or misappropriated cash is obscured by applying subsequent receipts to cover the first theft.

- Requires access to the finance software!
  - Alter the accounts receivable to obscure the stolen funds.
  - Delayed deposits
  - Must keep on it or the house of cards falls
  - Cannot share your job with anyone

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
- Employee appears stressed
- Employee living beyond their means.

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
- Highly encourage vacations and cross training
- Detailed reconciliation of monthly ledgers
  - Investigate trends of decreased cash despite sales remaining constant

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
    - Office Space
    - Vehicles
- Larceny
  - Purchasing and receiving schemes
  - Asset requisitions and transfers

UNIVERSITY of ALASKA
Many Traditions One Alaska

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 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

Three former Georgia Tech Researchers
Sentenced in Scheme to Defraud CIA

Chief Scientist for Georgia Tech Research Institute (GTRI) and two other researchers charged $200,000 on Procard for personal expenses from 2007 to 2013. Charged fraudulent purchases to GTRI contract funded by the CIA. In addition engaged in $696,000 of fraudulent consulting activities.

How they did it:

- Authorized to use Procard to purchase materials and supplies
- Used researcher's prior company as a billing pass-through
- Directed Georgia Tech employees to do work and charge effort to separate contract

How it was discovered:

- During routine audit discovered irregular Procard charges
- Researcher recorded cover up meeting

Outcome:

- Lost job and secret clearance
- Chief Scientist facing 5 years prison, pay 1.97 million in restitution

U.S. Attorney's Office Northern District of Georgia,
Justice.gov, November 1, 2023

Fraudulent Purchases and Consulting Activities

Red flags:

- Lack of proper supporting documentation
- Odd purchases for a grant or absence of physical equipment
- Prior reprimand for consulting activities
- Late sponsored program deliverables

What to monitor:

- Subrecipients functioning only as pass-through entities
- Effort reports that appear to “spend out a grant”

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 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
- Late support documents/refusal to submit 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!
- Link - 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
  - Criteria tailored to specific bidder
- Bribery schemes
  - Kickbacks

Fraud Cases in the News

- DoD employee used 60 fake student to apply for 6.7 million in aid from 2005 to 2021 which was disbursed to at least 8 colleges. He paid ghost writers based in Africa to log on and complete assignments.

Former Penn State employee sold $265,000 in computer equipment over 12 year period. Claimed equipment needed to upgrade, replace or maintain office servers.

New York college facility maintenance employee took bribes to award building construction, repair and maintenance contracts at the college.

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

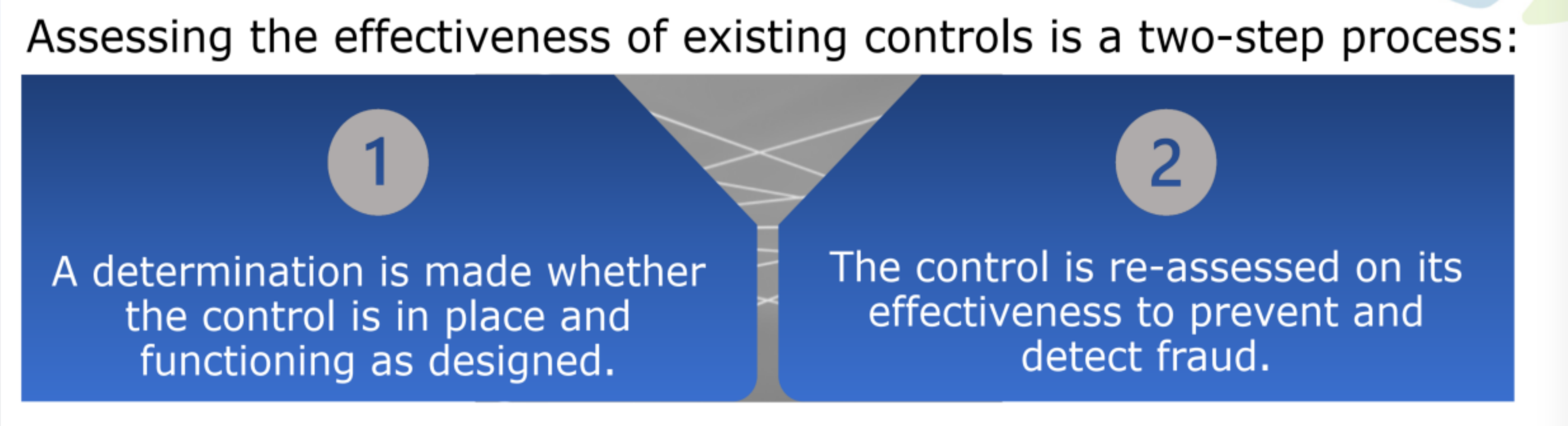
When in doubt do not open and do not respond the Phishing email!

Fraud Prevention: What can I do?

Fraud prevention starts with you!

Fraud Prevention

Something about Change is Constant



Assessing the effectiveness of existing controls is a two-step process:

1 A determination is made whether the control is in place and functioning as designed.

2 The control is re-assessed on its effectiveness to prevent and detect fraud.

Internal Controls can only be effective if:

- Intentionally designed
- Consistently applied
- Periodically reviewed

A. Vartanova, University of Colorado, ACUA AuditCon 2023

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 Purposeful Questions

- Professional skepticism

Make time for staff training

Periodically review company policies and procedures

- Capture changing processes and regulations

Report it to your supervisor, University Police, or General Counsel

Contact the Office of Audit and Consulting Services by phone or email

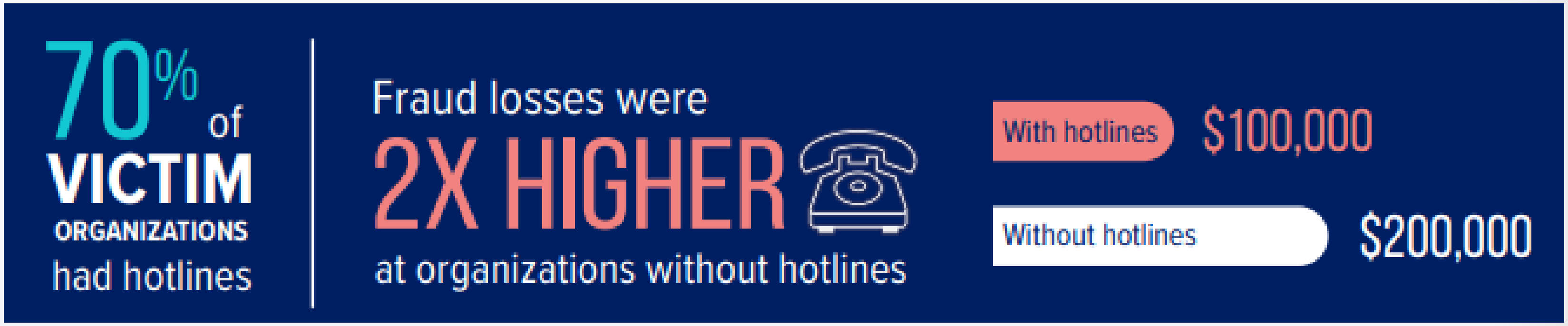
- Phone – 907-786-7756 or 907-450-8094
- Email – nrcountryman@alaska.edu or nlpittman@alaska.edu

Report your suspicions anonymously at:

- www.alaska.ethicspoint.com

UNIVERSITY *of* ALASKA
Many Traditions One Alaska

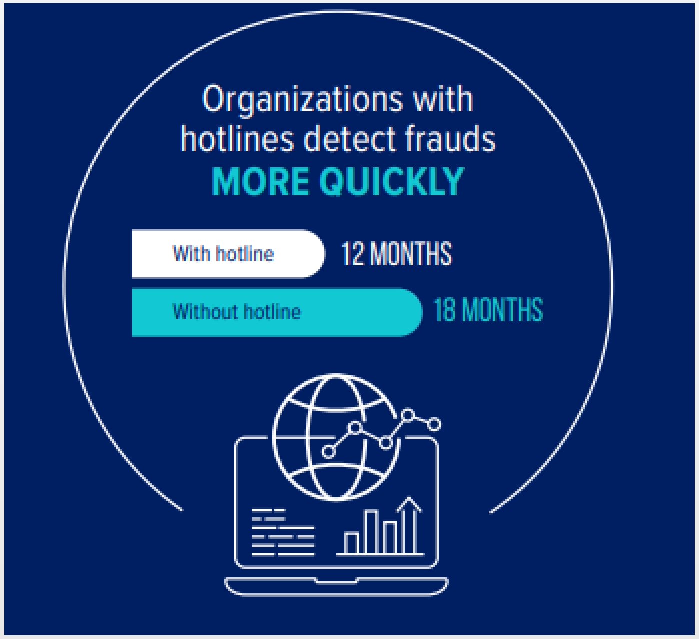
UA Confidential Hotline



70% of VICTIM ORGANIZATIONS had hotlines

Fraud losses were 2X HIGHER ☎ at organizations without hotlines

With hotlines	$100,000
Without hotlines	$200,000



Organizations with hotlines detect frauds MORE QUICKLY

With hotline	12 MONTHS
Without hotline	18 MONTHS

Association of Fraud Examiners 2022 Report to the Nations

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

UA Confidential HOTLINE Make the Right Call www.alaska.ethicspoint.com

UNIVERSITY of ALASKA
Many Traditions One Alaska

Presentation Resources and Works Cited

- 2022 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.
- Association of College and University Auditors
- Institute of Internal Auditors
- Fraud Mitigation in Remote Environment, A Vartanova, University of Colorado, 2023
- 2019 Fraud Examiner's Manual, ACFE, 2019.
- System Office of Audit and Consulting Services Website
  - A&CS Internal Controls - http://www.alaska.edu/audit/
  - Self-Assessment Questionnaires

University of Alaska System
Office of Audit and Compliance 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 the A&CS website at
http://www.alaska.edu/audit/

UNIVERSITY *of* ALASKA
Many Traditions One Alaska

Fraud Prevention

It Starts with You!

UNIVERSITY *of* ALASKA

Many Traditions One Alaska