Fraud Prevention

Chase Lenon, CPA, CGFM

Director of Audit Services

What is Fraud?

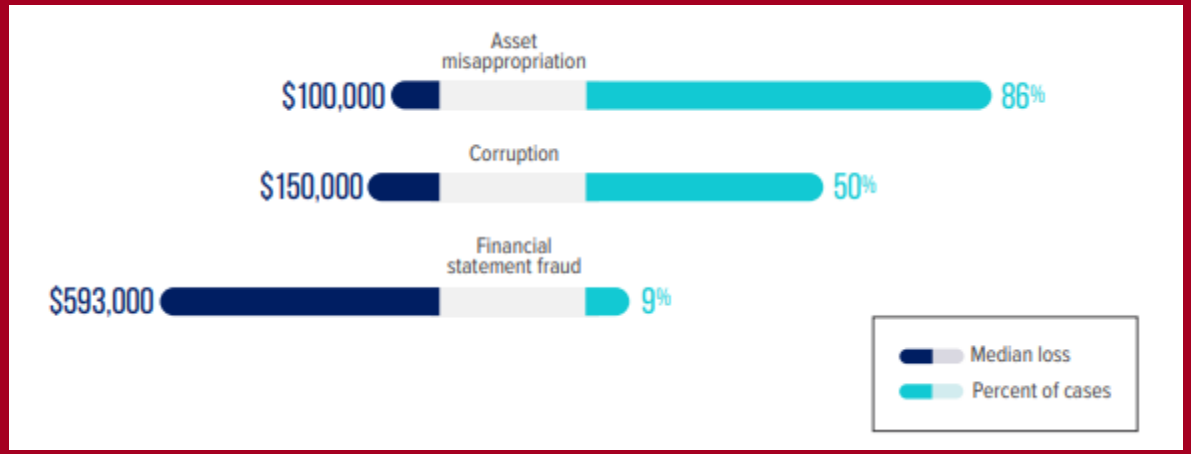
- Fraud is a deliberate act (or failure to act) with the intention of obtaining an unauthorized benefit, either for oneself or for the institution, by using deception or false suggestions or suppression of truth or other unethical means, which are believed and relied upon by others.

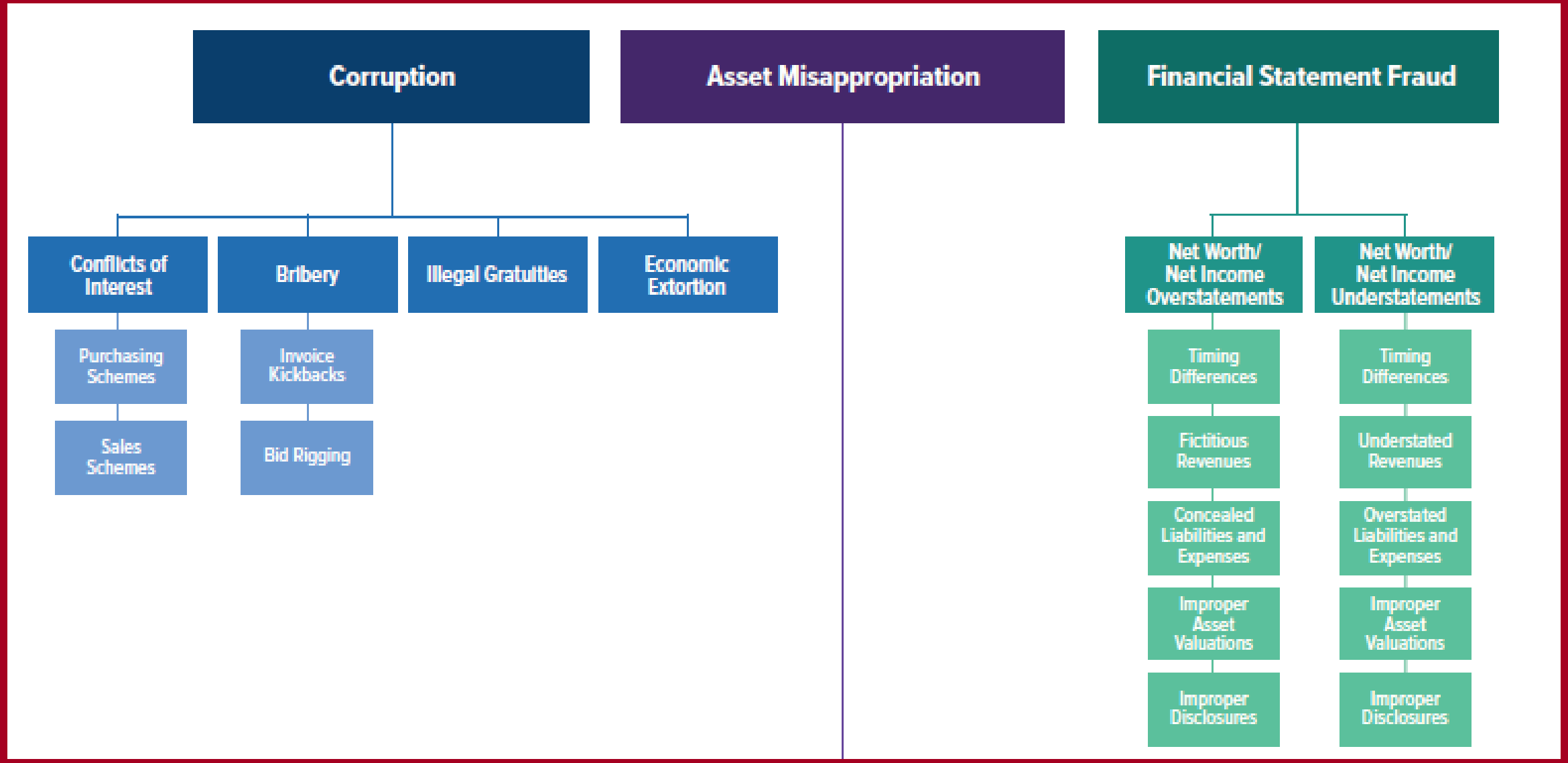
Why Commit Fraud?

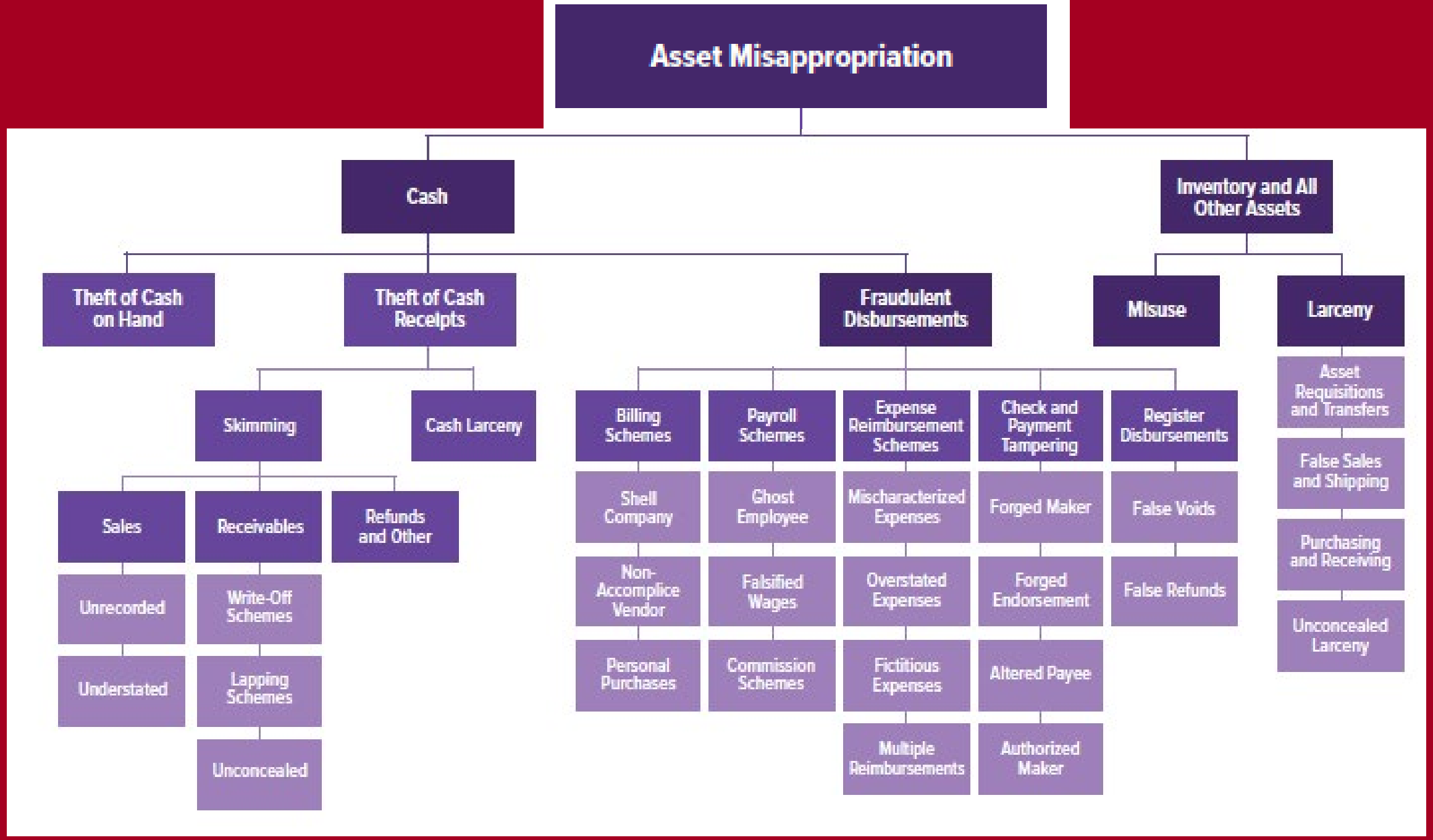
- Perceived Financial Need
- Perceived Opportunity
- Rationalization

3 Main Categories of Fraud

1. Asset Misappropriation
2. Corruption
3. Financial Statement Fraud




Corruption
Asset Misappropriation
Financial Statement Fraud
Conflicts of Interest
Bribery
Illegal Gratuities
Economic Extortion
Purchasing Schemes
Sales Schemes
Invoice Kickbacks
Bid Rigging
Net Worth/ Net Income Overstatements
Net Worth/ Net Income Understatements
Timing Differences
Fictitious Revenues
Concealed Liabilities and Expenses
Improper Asset Valuations
Improper Disclosures
Timing Differences
Understated Revenues
Overstated Liabilities and Expenses
Improper Asset Valuations
Improper Disclosures


Asset Misappropriation
Cash
Inventory and All Other Assets
Theft of Cash on Hand
Theft of Cash Receipts
Fraudulent Disbursements
Misuse
Larceny
Skimming
Cash Larceny
Billing Schemes
Payroll Schemes
Expense Reimbursement Schemes
Check and Payment Tampering
Register Disbursements
Asset Requisitions and Transfers
Sales
Receivables
Refunds and Other
Shell Company
Ghost Employee
Mischaracterized Expenses
Forged Maker
False Voids
False Sales and Shipping
Unrecorded
Write-Off Schemes
Non-Accomplice Vendor
Falsified Wages
Overstated Expenses
Forged Endorsement
False Refunds
Purchasing and Receiving
Understated
Lapping Schemes
Personal Purchases
Commission Schemes
Fictitious Expenses
Altered Payee
Unconcealed Larceny
Unconcealed
Multiple Reimbursements
Authorized Maker

Fraud Schemes

- Cash Receipt Schemes:
  - Skimming – removing cash BEFORE entry
  - Larceny – removing cash AFTER entry

- Concealing Receivables:
  - Lapping – taking customer A's money to use on customer B's account etc…

Fraud Schemes

- Fraudulent Disbursements
  - Forging checks, creating fake invoices, altering timecards.
  - Cash Register? Could falsely provide a refund or falsely void transactions.

- Expense Reimbursement Schemes
  - Mischaracterized, overstated, fictitious, or multiple expenses.

Fraud Schemes

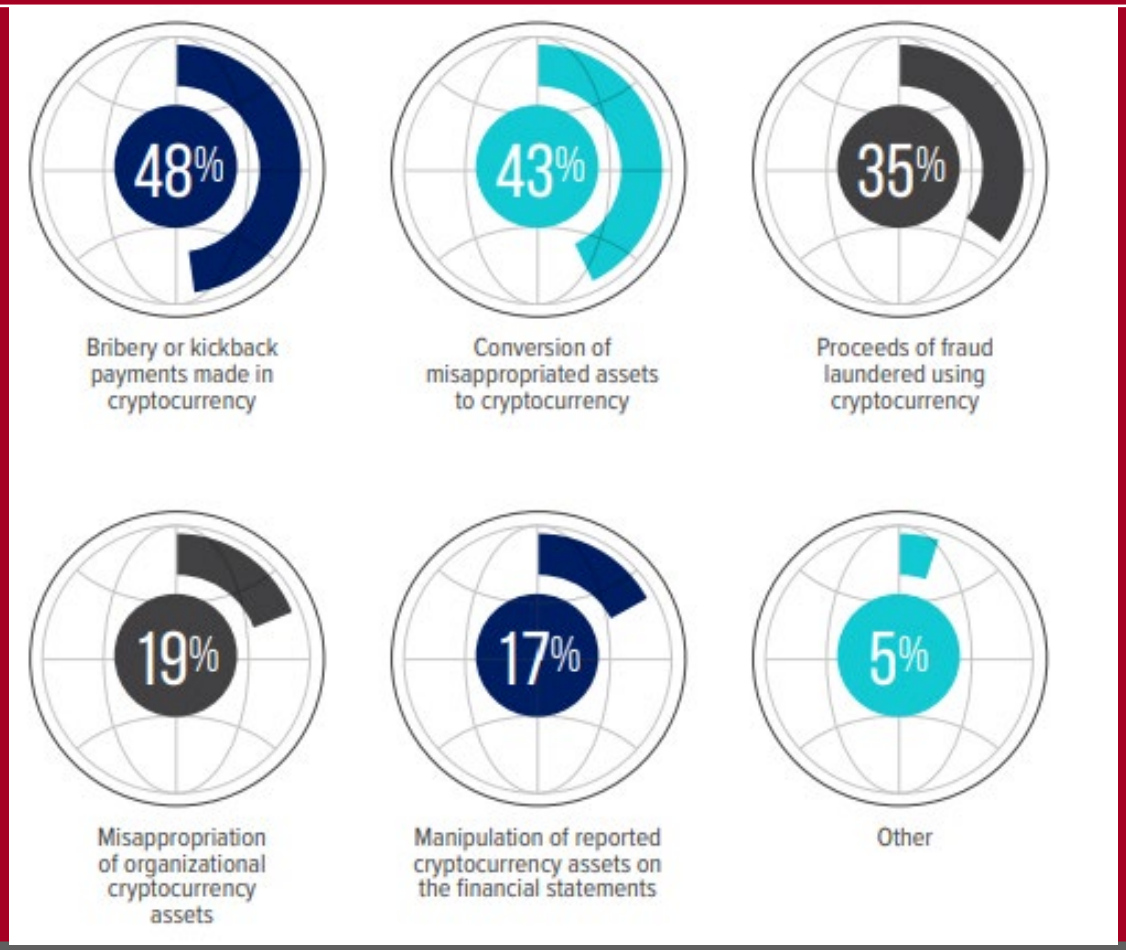
- Billing Scheme
  - False invoicing via shell companies via non-existent vendors (personal purchases).
- Payroll Schemes
  - Ghost employment, falsified hours, salary/commission combinations.

Fraud Schemes

- Bribery Schemes
  - Official (public) or Commercial (private).
  - Solicit corrupt payments to influence acts.
  - Illegal Gratuities - Items given to reward a decision (different than bribery – after the fact).

- Financial Statement Fraud Schemes
  - False entries.
  - False/unauthorized:
    - Transfers
    - Withdrawals
    - Disbursements
    - Disclosures

Cryptocurrency Schemes



Cryptocurrency

- Not considered “Legal Tender”.
- You might receive donations in Crypto. Treat as an unallowable investments (stocks).
- Unit equipment should not be used for personal use (mining) beyond de minimum limitations per local policies.
- We recommend consulting with the unit’s attorney on issues involving cryptocurrency.

Internet and Computer Fraud

- Fraud is growing exponentially in virtual spaces.

- SBOA IT Manual:
  - https://www.in.gov/sboa/files/Information-Technology-Manual-2017-Amended.pdf

Cybersecurity Tips

- Use antivirus software and enable Firewalls
- Keep software up-to-date
- Strong passwords and Multi-Factor Authentication
- Educate yourself on phishing scams (FTC Website)
- Protect Sensitive information (PII)
- Use equipment securely (cell phones, flash drives)
- Backup data regularly
- Do not use Public Wi-Fi
- What do during and after a cyber attack? https://www.ready.gov/cybersecurity

Disaster Recovery Plans

- Written plan with detailed instructions on how to respond to natural disasters, cyber-attacks, or other disrupting events.
- Should include procedures to back-up financial data frequently.
  - Storing data in a secure location not connected to main network is ideal.
  - Plan should include procedures to test backup data.
- Antivirus software and security patches should be up to date to prevent cyber-attacks.
- The Indiana Office of Technology (IOT) has many resources available.

2021 HEA 1169 - Cybersecurity Incidents

- Requires the office of technology to maintain a repository of cybersecurity incidents. Provides that a state agency and a political subdivision shall: (1) report any cybersecurity incident to the office without unreasonable delay and not later than two business days after discovery of the cybersecurity incident in a format prescribed by the chief information officer; and (2) provide the office with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident before September 1, 2021, and before September 1 of every year thereafter. Allows the office of technology to assist a state agency with certain issues concerning information technology. Provides that if requested by a political subdivision, the office may develop a list of third-party technology providers that work with the office. Requires a state educational institution to submit a quarterly analysis with certain conditions

Reporting Cybersecurity Incidents

- A cybersecurity incident may consist of one or more of the following categories of attack vectors: (1) Ransomware, (2) Business email compromise, (3) Vulnerability Exploitation, (4) Zero-day exploitation, (5) Distributed denial of service, (6) Web site defacement, (7) Other sophisticated attacks as defined by the chief of information officer and that are posted on the officer's Internet web site. (IC 4-13.1-1-1.5)

- Cybersecurity incidents can be reported on IOT's web site at the following webpage. https://www.in.gov/cybersecurity/report-a-cyber-crime/

Indiana Office of Technology – Local Government Services

- The Indiana Office of Technology (IOT) provides services to local units of government.

- Website services
  - FREE* - offers for a small monthly fee: website support, online payment processing, analytics/3rd party tools, application development…
- Email services
  - Secure /w @in.gov domain
- QPAs Assistance
  - Purchasing through State approved Contractors, hardware, software, telecom needs
- Cybersecurity Consulting
  - Response assistance
- Geographic Information System (GIS) services

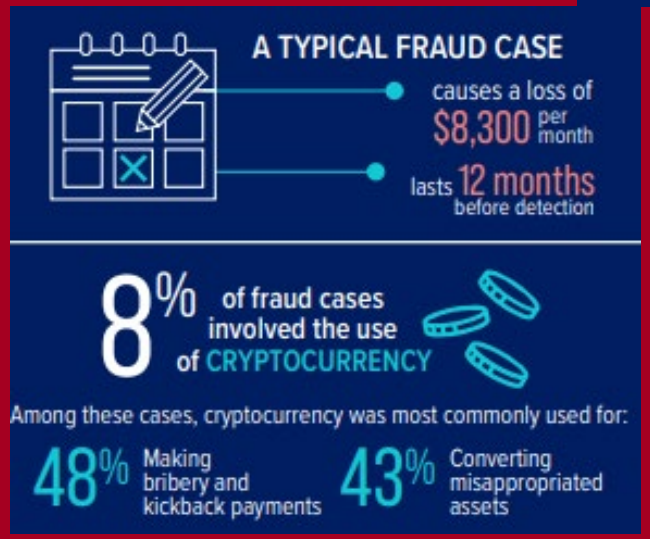
- https://www.in.gov/sboa/files/iot-services-3-24-22.pdf

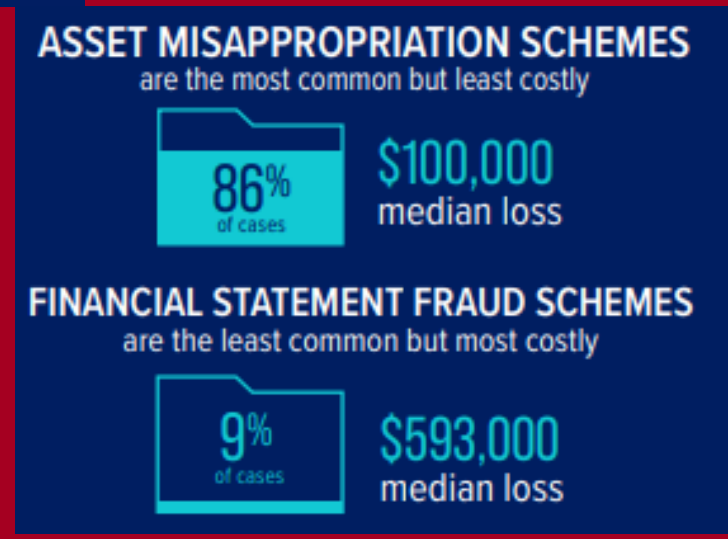
Fraud Statistics

Source

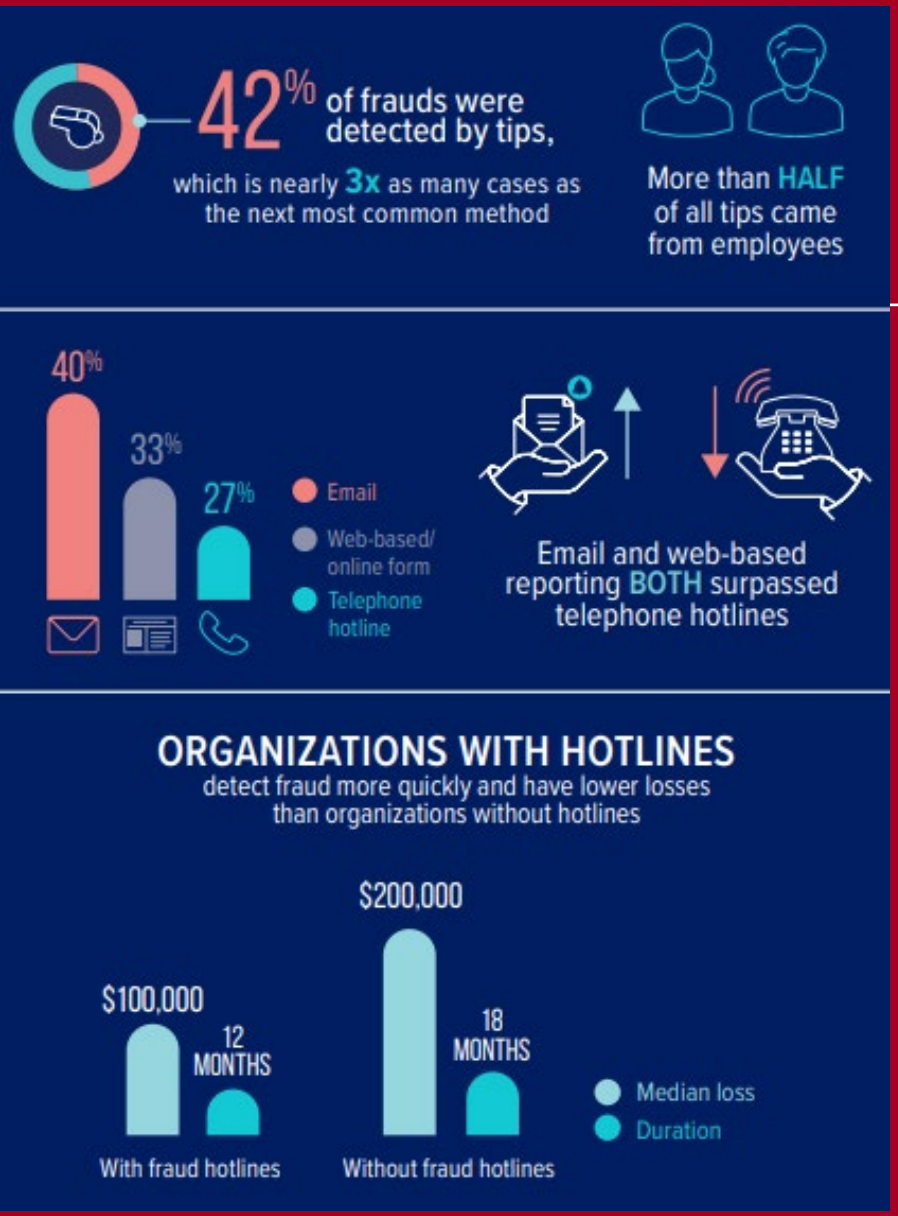
- *Report to the Nations*
  - *2022 Global Study on Occupational Fraud and Abuse*
  - *Published by: The Association of Certified Fraud Examiners*
  - *Report: https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf*

Key Findings





Key Findings Continued

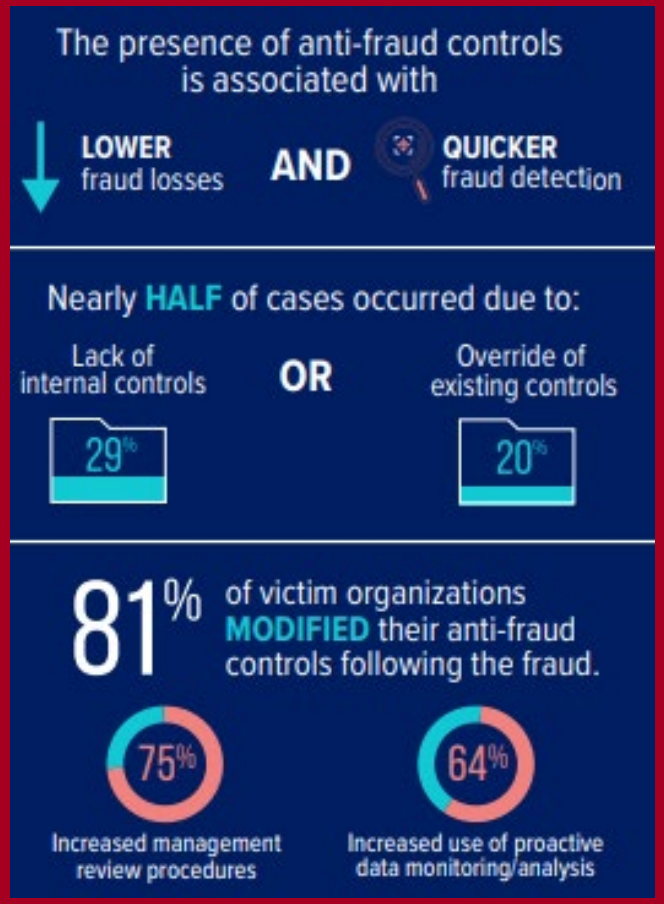


These five have **INCREASED** the most:

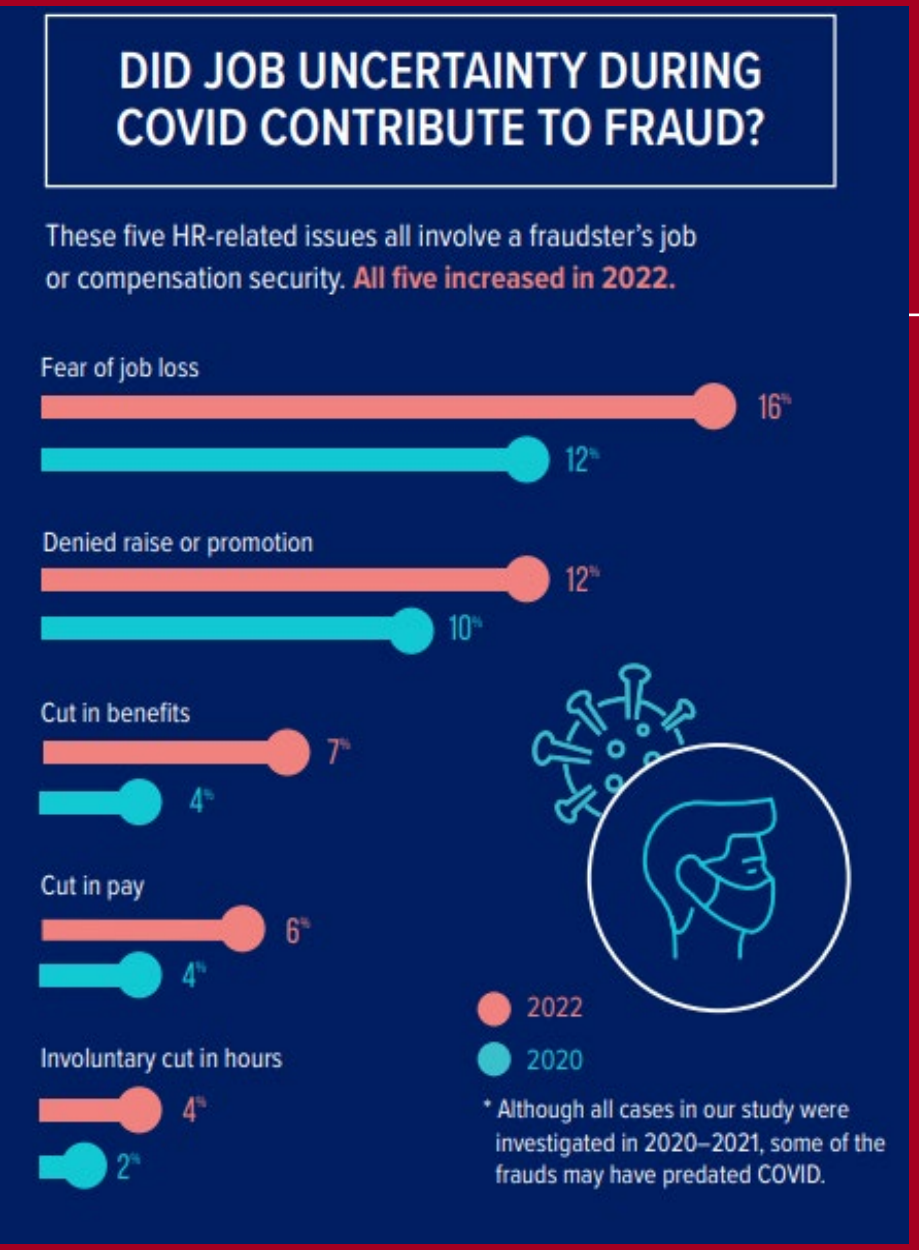
	2012	2022	Increase
Hotline	54%	70%	16%
Fraud training for employees	47%	61%	14%
Anti-fraud policy	47%	60%	13%
Fraud training for managers/ executives	47%	59%	12%
Formal fraud risk assessments	36%	46%	11%

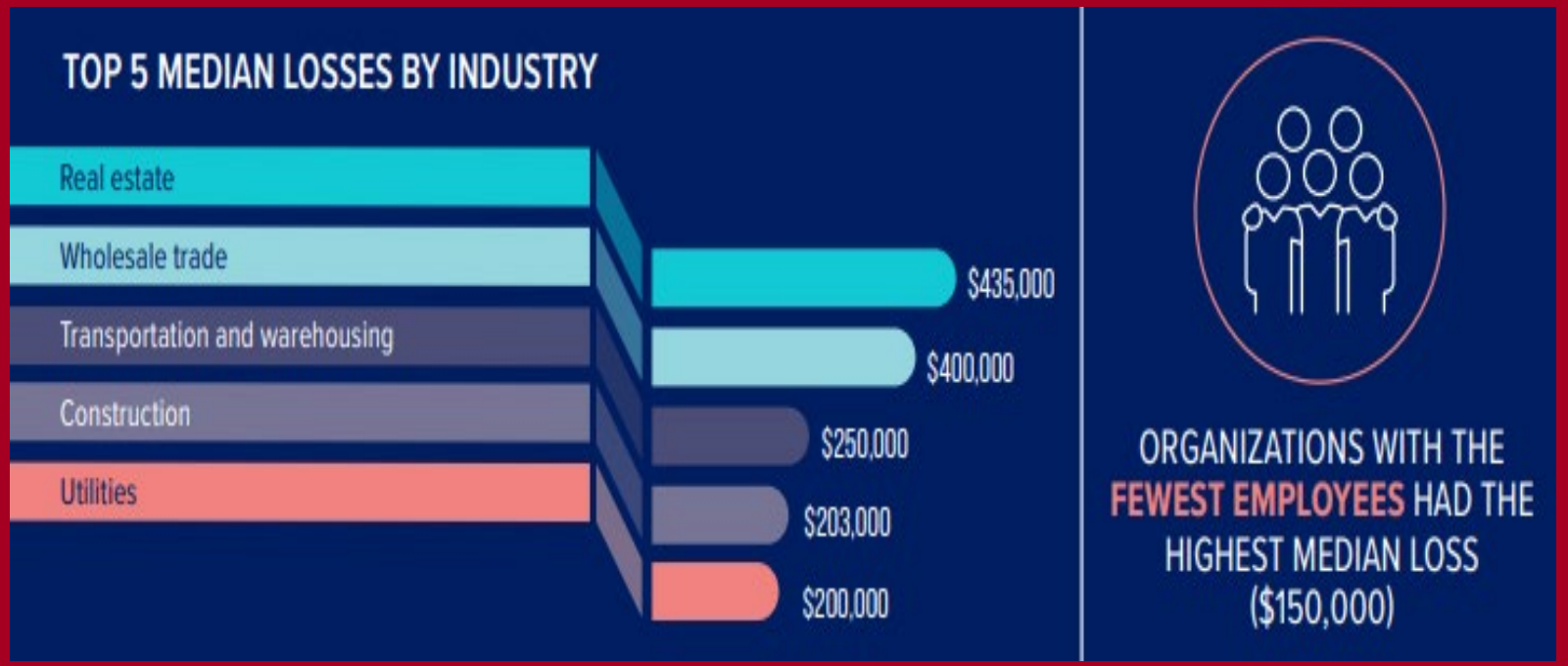
CORRUPTION
was the most common scheme in every global region

Key Findings Continued

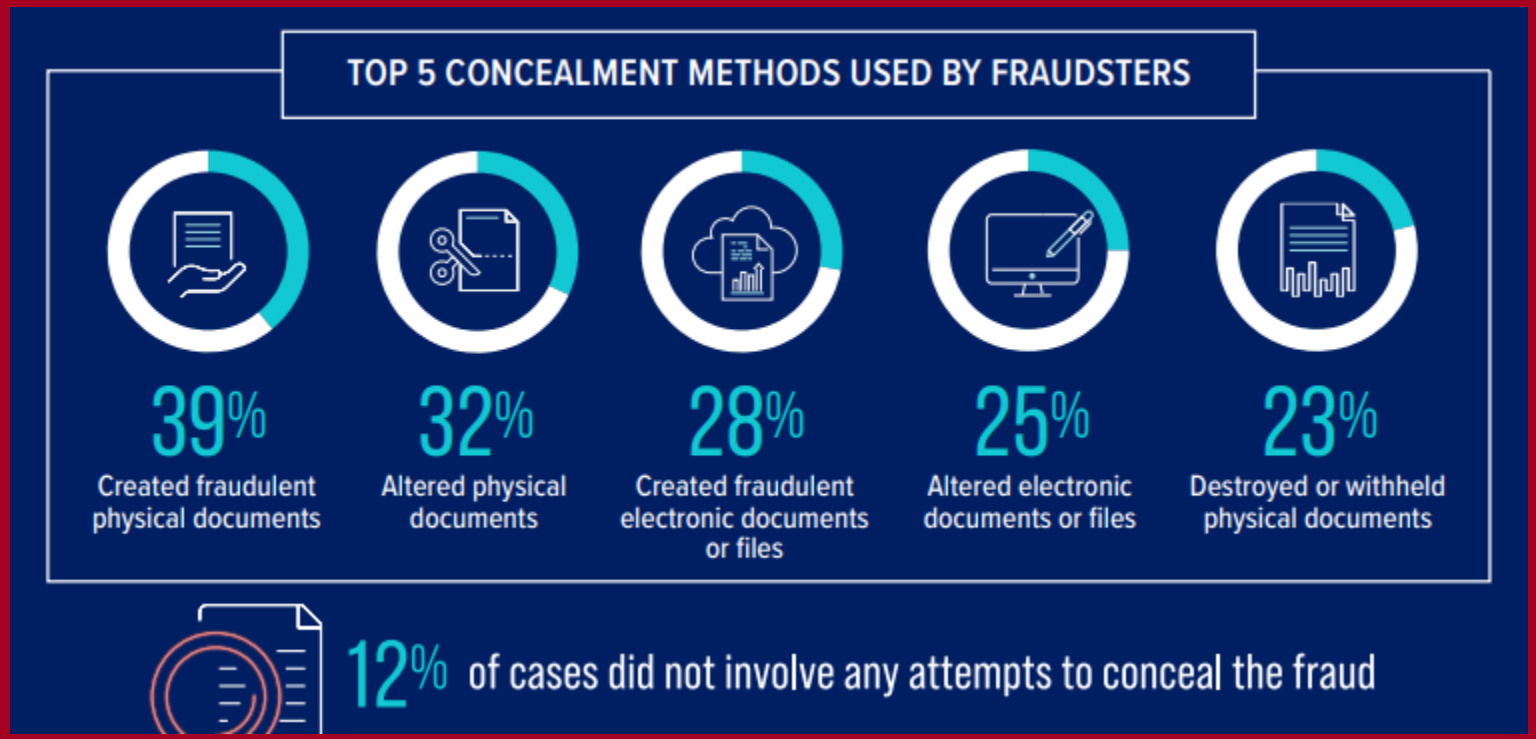


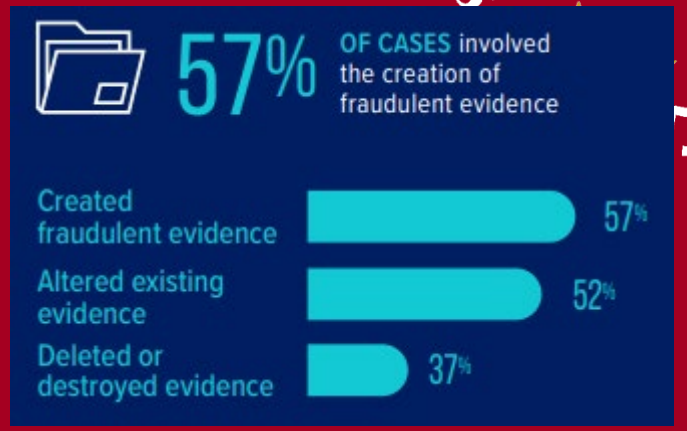
Key Findings Continued

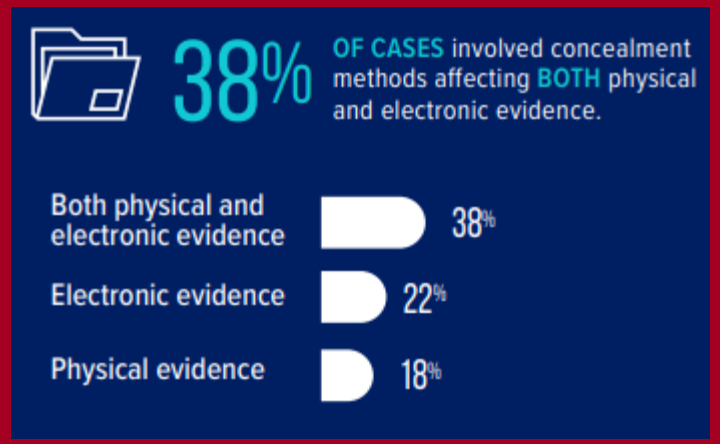


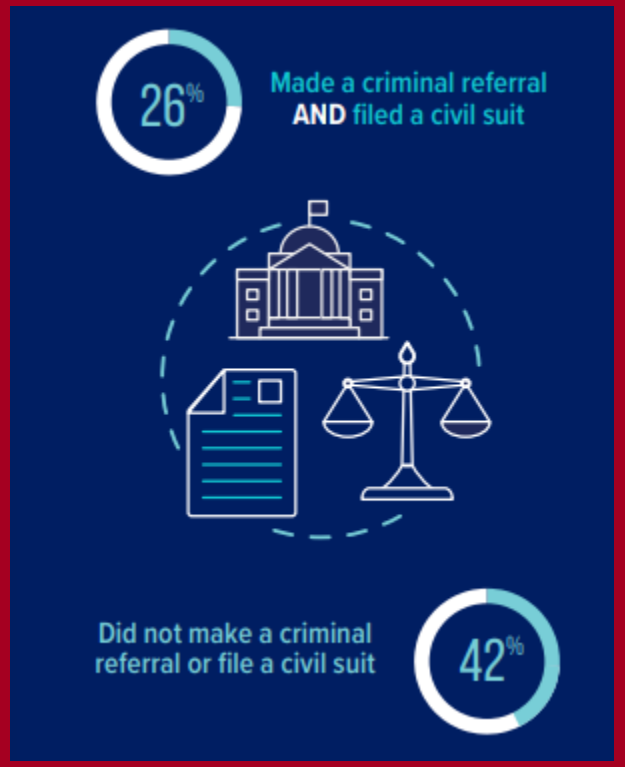


How is Fraud Concealed?

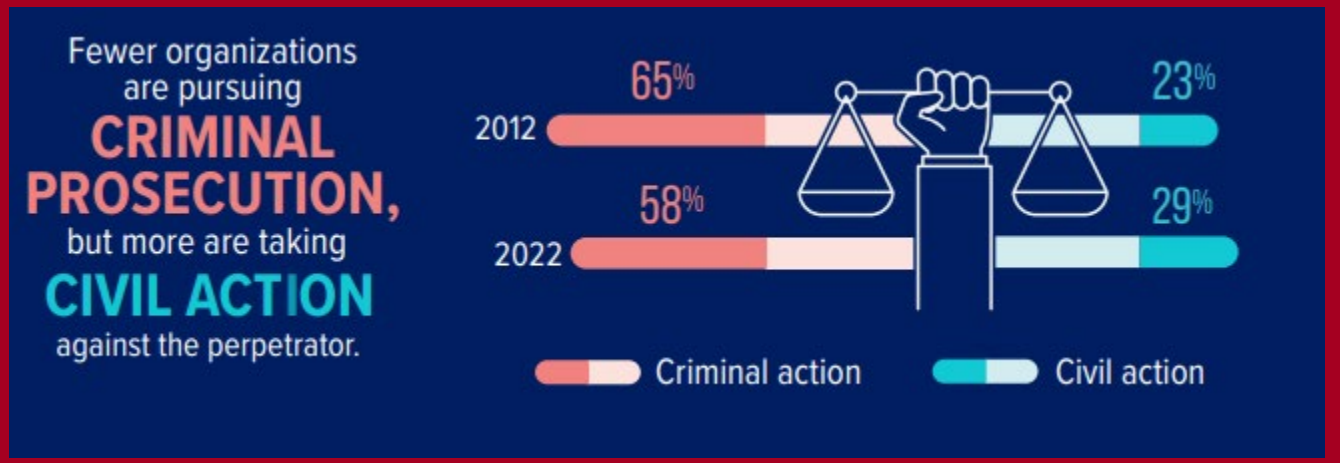






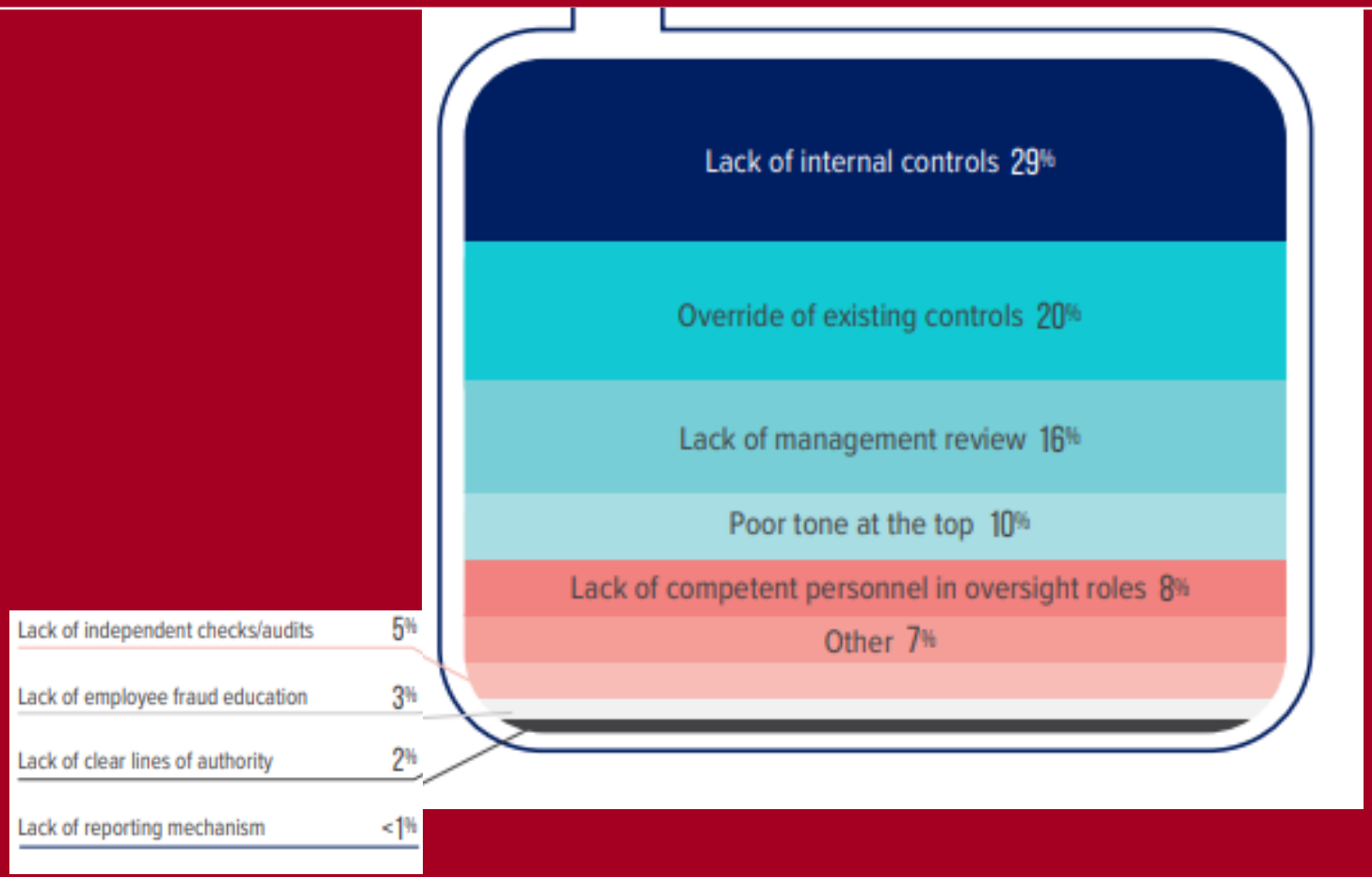


- Responses to Fraud



Fraud Prevention

What Contributes to Fraud?



- Primary weakness contributing to fraud?
- Lack of controls!!!

Components of Internal Control

- **C**ontrol Activities
  - Actual procedures performed
- **R**isk Assessment
  - Where could things go wrong?
- **I**nformation and Communication
  - If things go wrong, do you know?
- **M**onitoring
  - It needs to be continuous process
- Control **E**nvironment
  - 'Tone at the top'

C.R.I.M.E!

Risky Areas to Assess

- Receipt/Payment Transactions
- Financial Reporting
- Federal Grants
- Security of Assets
- Payroll
- Vendor Payments
- Fundraising activities

Trust is not a control!

- Do you have someone at your unit who is very knowledgeable about processes and no one else knows how certain things work?

- Someone else should understand and review!

Types of Controls

- ***Preventative controls*** are those such as requiring dual signatures on checks or having password-protected files. This type of control protects and limits access to assets.

- ***Detective controls*** include reconciling the bank or inventory counts. Typically, these internal controls are performed periodically to see if any need to be corrected. They will often turn up internal errors or problems, as well as any external errors (such as bank errors).

Detection

- If you identify errors (or fraud) early, then you can mitigate the damage!!

- Allows for improvements to detect and deter fraud.

Detective Controls

- Avenue to report:
  - Hotlines, email, online form etc….
- Internal “Audits”
- Management Review of periodic processes
  - Bank reconcilements
  - Physical inventory checks
  - Cash change and sales reports (such as ticket sales on the SA-4)
- Proactive Data Monitoring
  - Analytical reviews, Reasonableness testing etc…
- Review equipment usage

FIG. 10 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

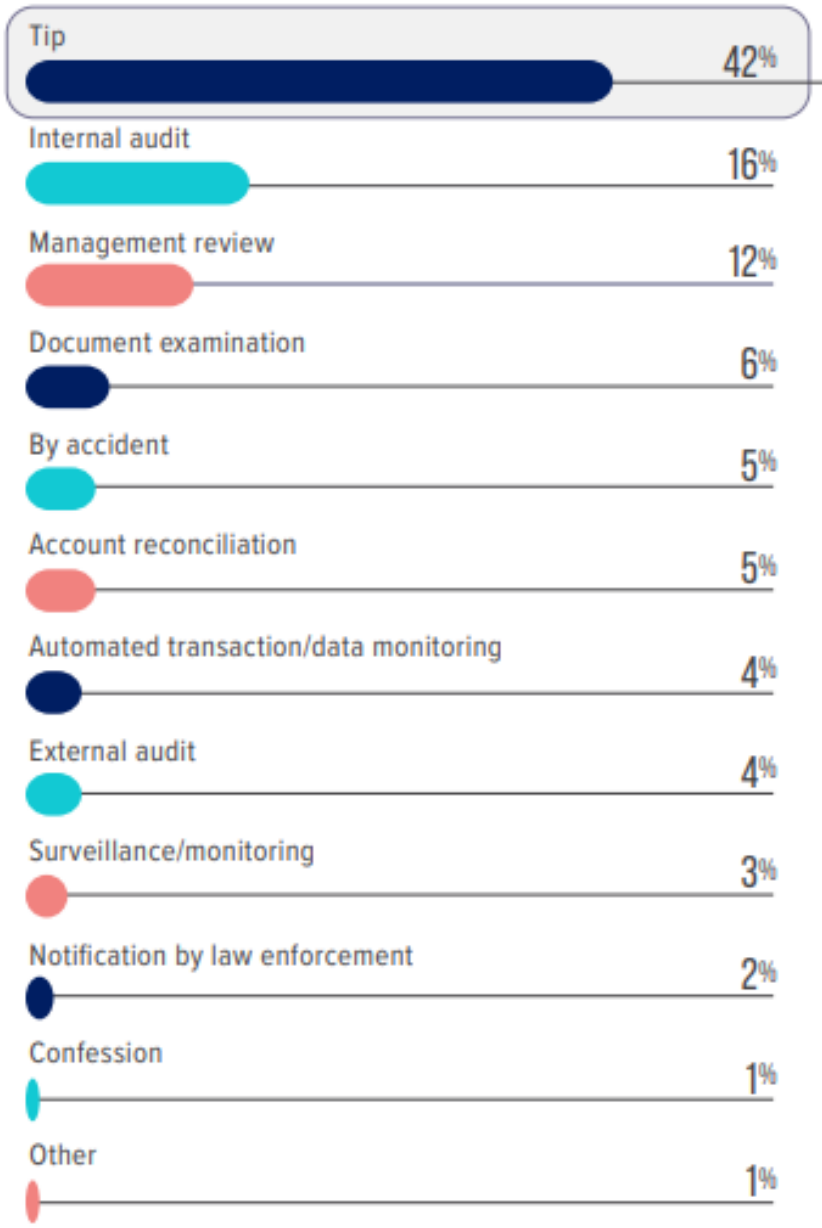
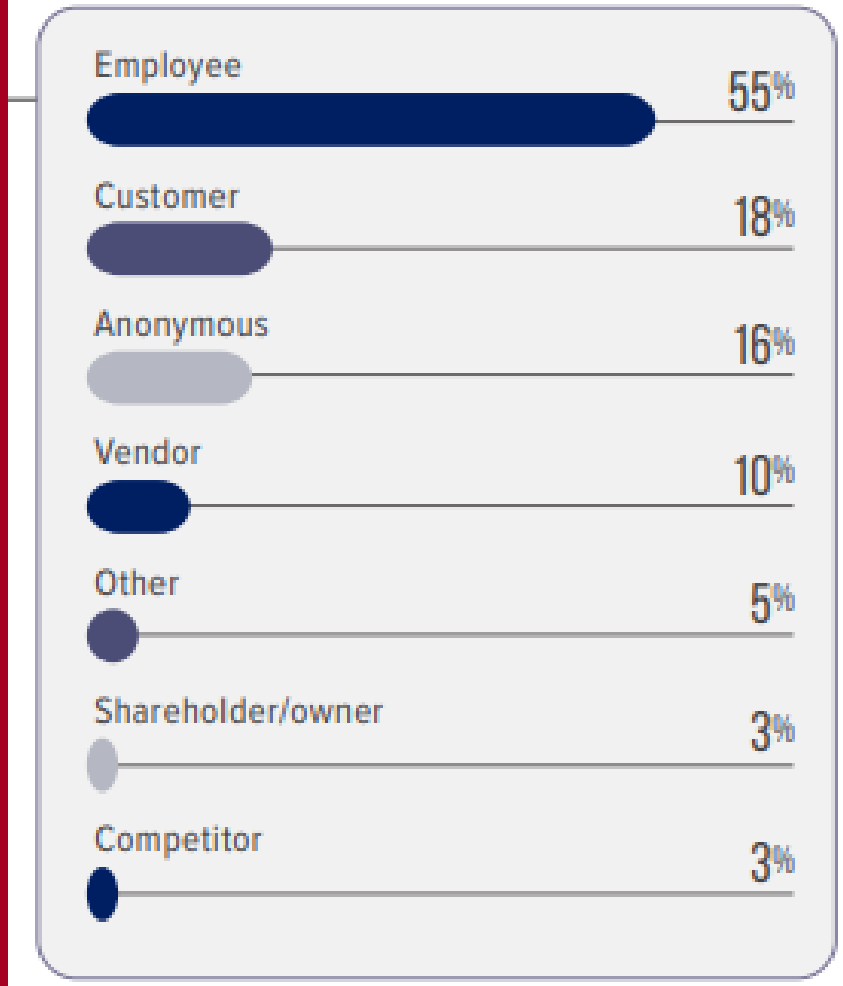


FIG. 11 WHO REPORTS OCCUPATIONAL FRAUD?



Preventive Controls

- Fraud Prevention Training
- Anti-Fraud Policy (code of conduct)
- Job Rotation/Mandatory vacation
- Safeguarding Assets
- Verify Vendor Legitimacy

- Monitor if policies and procedures are being followed
  - Determine if sufficient to address risk
  - Determine if changes in environment (or individuals) require changes

Prevention Recommendations

- Ensure no one person has control over all parts of a transaction.
- Restrict use of agency credit cards and verify all charges made.
- Protect checks against fraudulent use.
- Protect cash and check collections.

Prevention Recommendations

- Review the use of position to waive fees or to not charge for services.
- Review the use of unit's credit card and policy.
- Review overpayments of salaries.
- Be aware of possible kickbacks, bribery, pay-to-play schemes.

Segregation of Duties

- Duties that “should” be separated:

- *Receipt roles* - Collecting, Depositing, Recording and Reconciling functions.

- Purchasing roles – Ordering, Receiving, Claim Creation/Approval, Payment, and Reconciling functions.

- *Inventory roles* - Requisition, Receipt, Disbursement, Conversion to scrap and Receipt of scrap proceeds functions.

Duties	Employee Number							
	1	2	3	4	5	6	7	8
Cash Receipts								
1. Open mail and write receipt								
2. Receive money, issue official receipts								
3. Take off cash register totals								
4. Balance cash drawer or cash register								
5. Make up bank deposits								
6. Take deposits to bank or remit to receiving officer								
7. Post receipts								
8. Access to computer system to make adjustments								
9. Approves adjustments								
10. Post credits to accounts receivable								
11. Prepare customer billings								
12. Mail billings or statements								
13. Approve bad debt write offs								
14. Approve accounts receivable adjustments								
15. Issue permits, licenses, etc.								
16. Issues receipts for electronic deposits								

Cash Disbursements

1.	Authorize purchases							
2.	Prepare purchase orders							
3.	Certify receipt of goods or services							
4.	Audit claims							
5.	Approve claims - Disbursing Officer							
6.	Approve electronic transfers							
7.	Write checks							
8.	Initiate electronic transfers							
9.	Post checks							
10.	Sign checks - Control of signature stamp							
11.	Mail or distribute checks							
12.	Custodian of petty cash							
13.	Custodian of investments							
14.	Access to check stock							
15.	Access to computer system to make adjustments							
16.	Approves adjustments							

Payrolls

1.	Post vacation and sick leave records							
2.	Check and extend time cards							
3.	Prepare payroll claims							
4.	Approve payroll claims for department							
5.	Approve payroll claims for disbursing officer							
6.	Calculate deductions and net pay							
7.	Write payroll checks							
8.	Sign payroll checks							
9.	Distribute payroll checks							
10.	Prepare earnings and deductions reports							
11.	Prepare W-2s and compare to earnings records							
12.	Access to computer system to make adjustments							
13.	Approves adjustments							

Cash

1. Receives bank statement in mail and opens it
2. Compares checks cleared to disbursements posted
3. Compares deposits to receipts posted
4. Prepares bank reconcilement
5. Approves bank reconcilement

Statement of Expenditures of Federal Assistance

1. Enters grant information into Gateway
2. Approves grant information entered in Gateway
3. Approves the prepared SEFA

Financial Close and Reporting

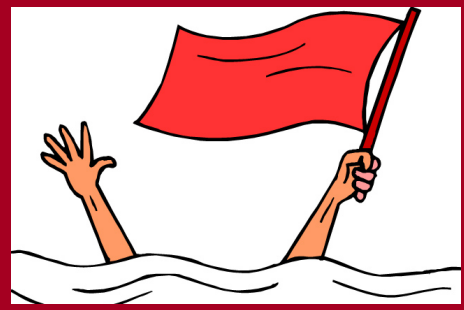
1. Closes the financial records
2. Enters financial statement information into Gateway
3. Approves the Gateway annual report
4. Approves the prepared financial statements

Notes to the Financial Statements

1. Enters the required information into Gateway
2. Approves the notes to the prepared financial statements

Red Flags

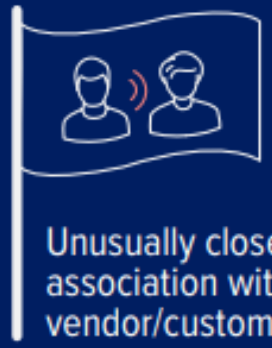
- Living beyond means
- Financial difficulties
- Close vendor relationship
- Unwilling to share duties
- Irritable/defensiveness
- Problems at home
- Complained about pay
- Refusal to take vacations
- Excessive pressure within
- Past employment issues
- Legal problems
- Wanting more authority
- Excessive peer pressure
- Instability in life
- Bullying/Intimidation
- Poor evaluation
- Wheeler-dealer attitude
- Social Isolation



These 6 RED FLAGS were much more common among long-tenured employees

Living beyond means

36% 43%



Unusually close association with vendor/customer

17% 25%

Control issues, unwillingness to share duties

11% 19%

Bullying or intimidation

11% 15%

Irritability, suspiciousness, or defensiveness

12% 15%

Recent divorce or family problems

10% 15%

≤5 years >10 years

State Examiner Directive 2015-6

- Materiality threshold for reporting irregular variances, losses, shortages, and thefts.
  - https://www.in.gov/sboa/files/Directive_2015-6.pdf
- Must notify SBOA and County Prosecutor.
- No materiality threshold for Fraud.

1. Is ongoing anti-fraud training provided to all employees?

- Do employees understand what fraud is?
- Have the consequences of fraud been made clear?
- Do employees know where to seek advice on potential unethical situations?
- Has a zero-tolerance policy been communicated through words/actions?

2. Is an effective fraud reporting mechanism in place?

- Do employees know how to use?
- Is there more than one reporting channel?
- Do employees trust reports are confidential?
- Has it been made clear that reports will be acted upon promptly?
- Do reporting policies extend to external parties?

3. To increase employees' perception of detection, are these measures being taken?

- Is fraud sought out rather than dealt with passively?
- Are internal surprise audits performed?
- Are data analytics used to identify variances?
- Are controls reviewed and monitored?

4. Is management's tone at the top one of honest and integrity?

- Are employees surveyed to determine if management acts with integrity?
- Are performance goals realistic?
- Have fraud prevention goals been identified?
- Has there been internal control policies implemented and tested?

5. Are fraud risk assessments performed to proactively identify and mitigate the company's vulnerabilities to fraud?

6. Are strong anti-fraud controls in place and operating effectively?

- Proper Segregation of Duties
- Use of Authorizations
- Physical Safeguards
- Job Rotations
- Mandatory Vacations

7. Does the internal audit department, if one exists, have adequate resources and authority?

- Important to operate without undue influence from management

8. Does the hiring policy include:

- Past employment verifications
- Criminal and civil background checks
- Credit checks
- Drug screening
- Education Verification
- Reference checks

9. Are employee support programs in place to assist with employees struggling with:

- Addiction
- Mental/Emotional Health
- Family problems
- Financial Problems

10. Is an open-door policy in place that allows employees to speak freely about pressures?

11. Are regular, anonymous surveys conducted to assess employee morale?

Contact Information

Chase Lenon, CPA

Director of Audit Services

Schools.Townships@sboa.in.gov

317-232-2512

Questions?