



Mitigating Big Risks for Small Businesses

Introduction



Neely Duncan

Partner

Forvis Mazars

214.293.7166

Neely.duncan@us.forvismazars.com

Key Take Aways



Understand key areas of small business organizations to consider for risks & compliance



Understand what needs to be considered to protect your organization



Understand the impact of various operational areas to ensure an efficient & effective organization

Facts About Fraud: 2024 ACFE Report to the Nation

- Estimated that typical organization loses **5%** of its annual revenue
- **\$3.1 billion** was the total loss caused by the cases in the study
- The median loss per case was **\$146,000**
- **43%** of frauds were detected by tip
- Median losses for frauds by owners/executives were more than **7X** greater than those carried out by employees
- More THAN HALF of occupational frauds occur due to a lack of internal controls (**32%**) or an override of internal controls (**19%**)

FIG. 2 HOW IS OCCUPATIONAL FRAUD COMMITTED?

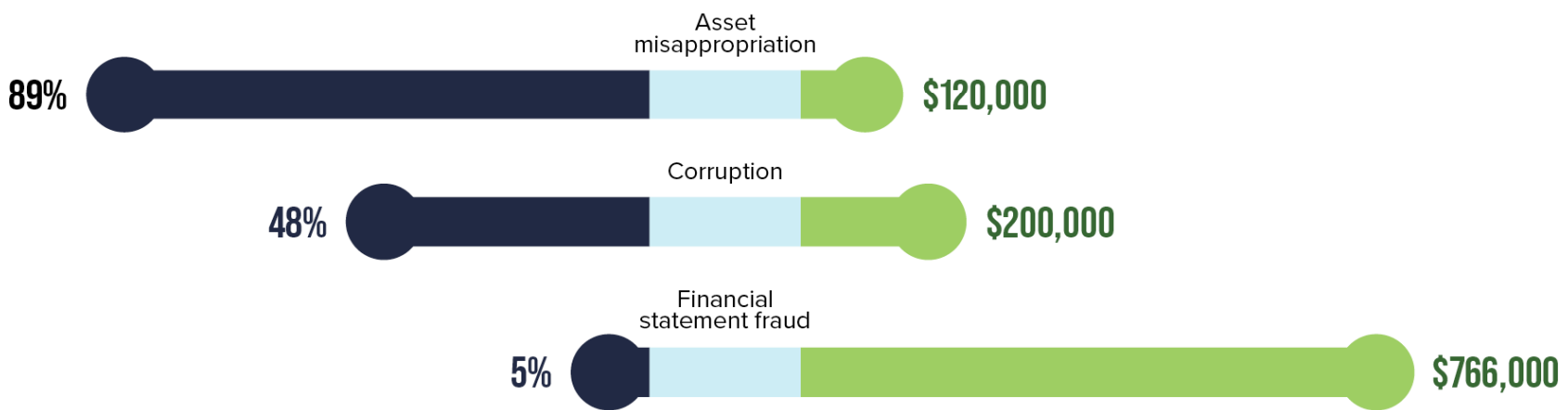
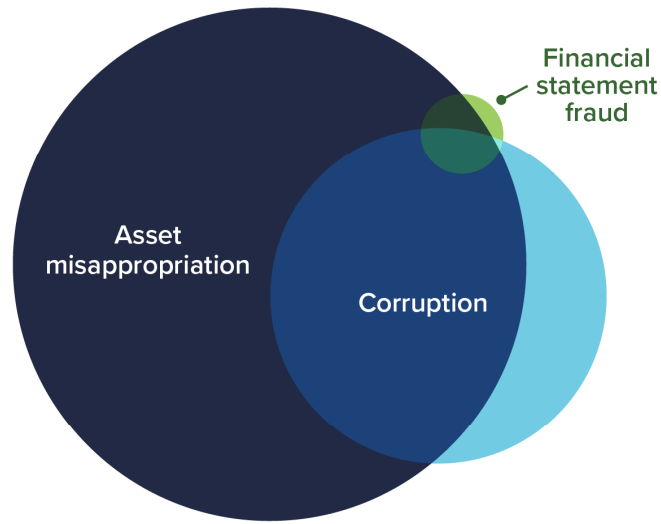


FIG. 4 HOW OFTEN DO FRAUDSTERS COMMIT MORE THAN ONE TYPE OF OCCUPATIONAL FRAUD?



Asset misappropriation only	51%	●
Asset misappropriation and corruption	35%	● ●
Corruption only	10%	●
Corruption, asset misappropriation, and financial statement fraud	2%	● ● ●
Asset misappropriation and financial statement fraud	1%	● ●
Financial statement fraud only	1%	●
Corruption and financial statement fraud	<1%	● ●

FIG. 25 HOW DOES OCCUPATIONAL FRAUD AFFECT ORGANIZATIONS IN DIFFERENT INDUSTRIES?

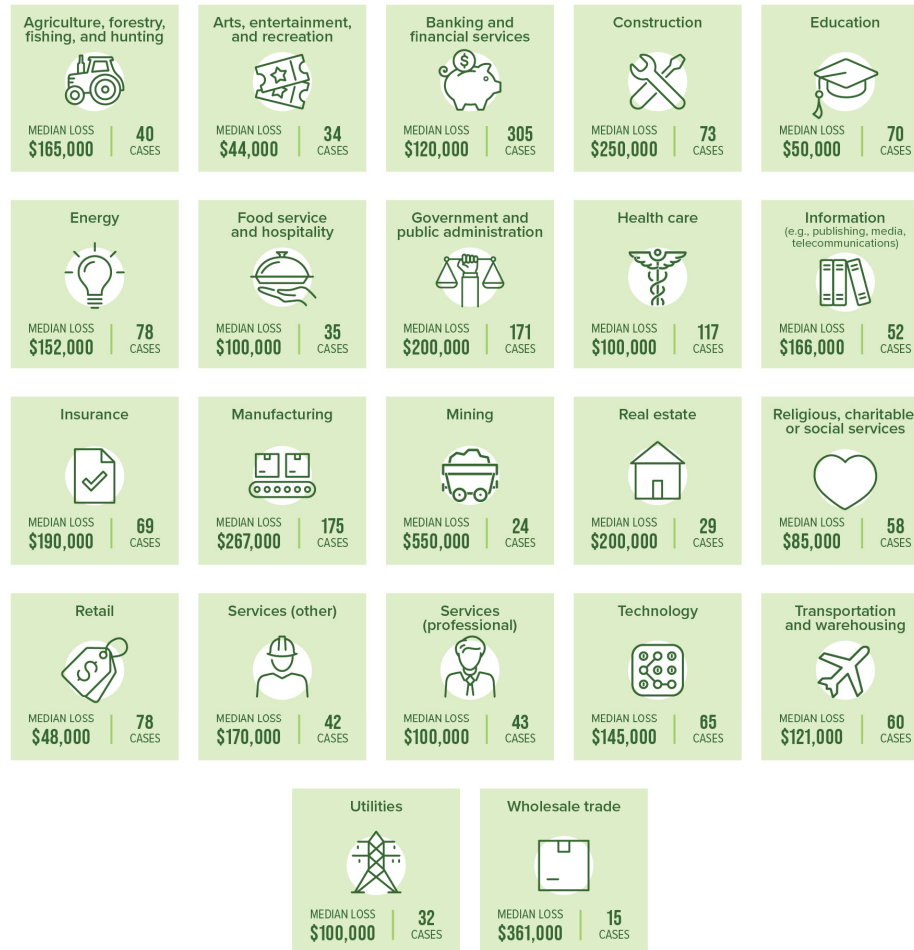
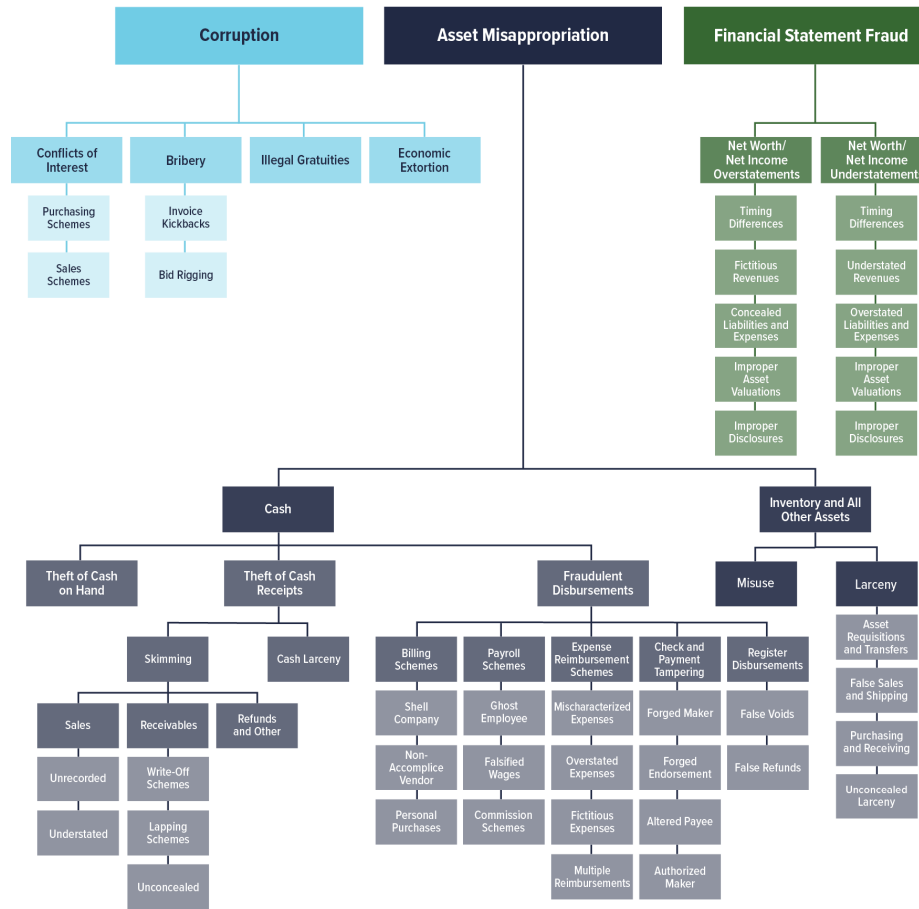
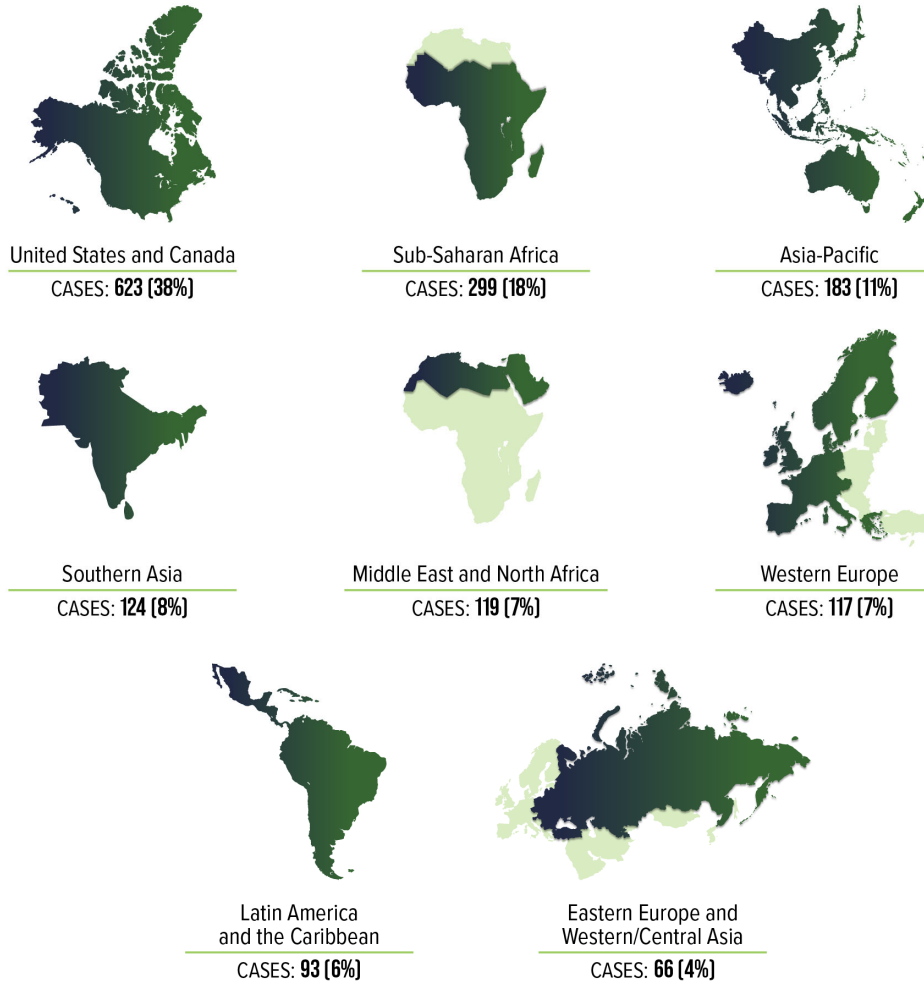


FIG. 3 OCCUPATIONAL FRAUD AND ABUSE CLASSIFICATION SYSTEM (THE FRAUD TREE)³



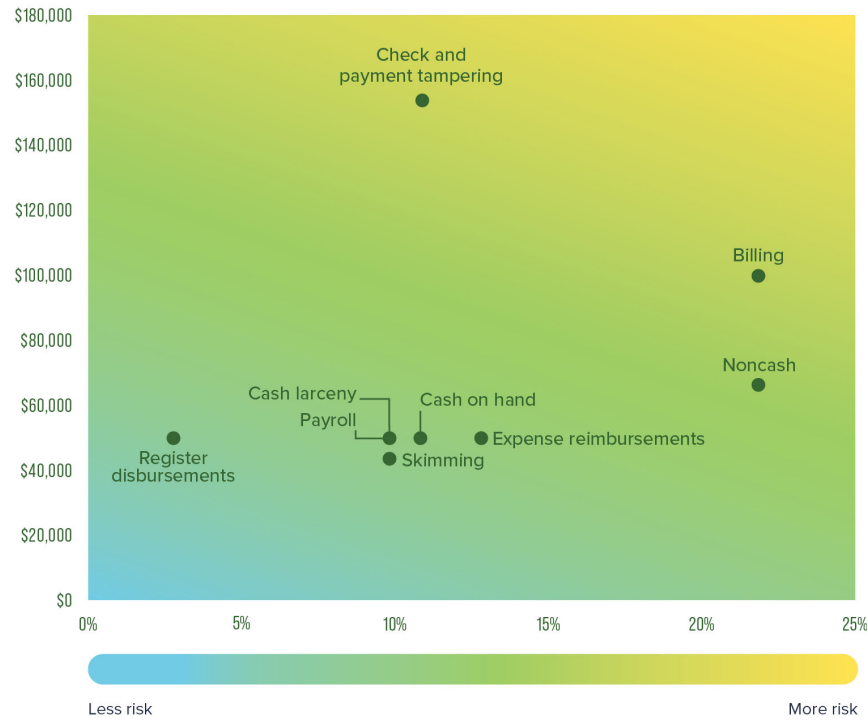
³The definitions for many of the categories of fraud schemes in the Fraud Tree are found in the Glossary of Terminology on page 104.

FIG. 1 REPORTED CASES BY REGION



Facts About F

FIG. 5 WHICH ASSET MISAPPROPRIATION SUB-SCHEMES PRESENT THE GREATEST RISK?

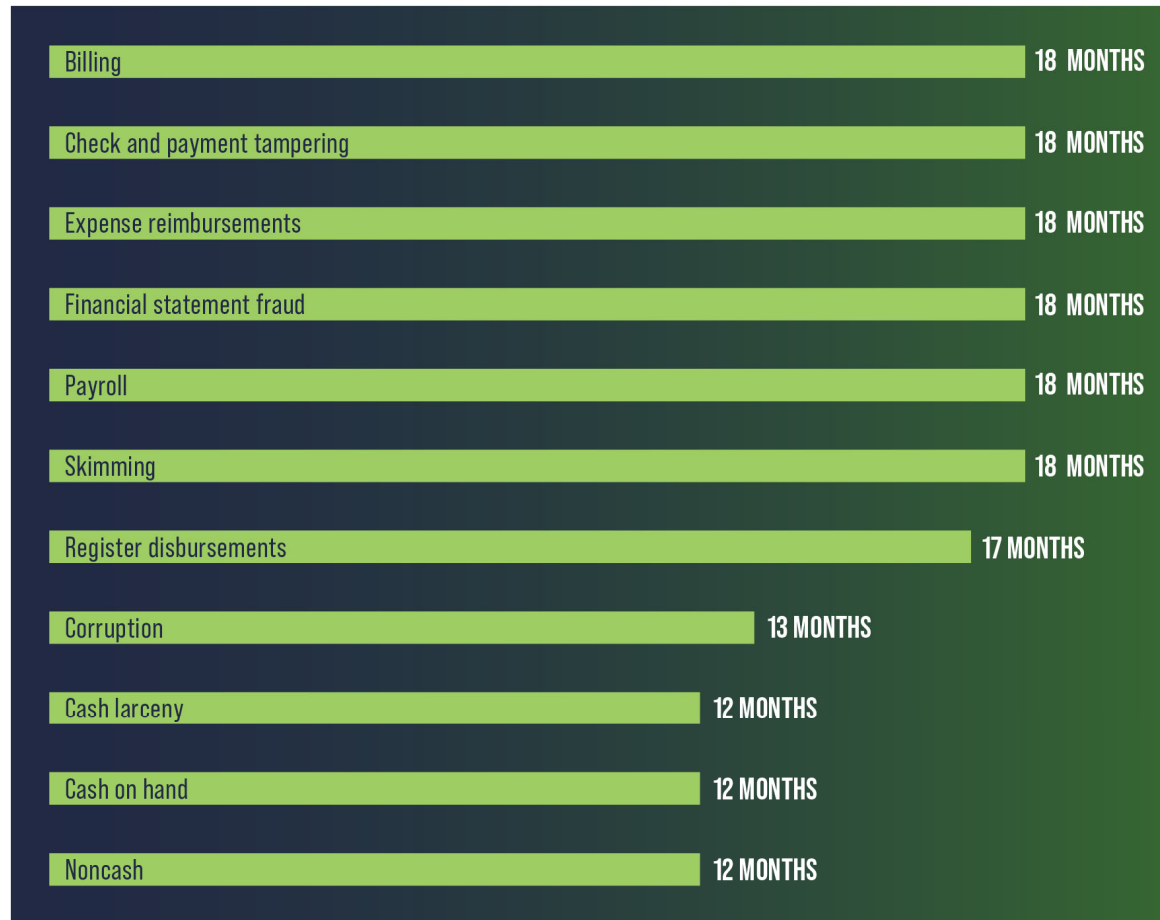


Which asset misappropriation schemes present the greatest risk?

Category	Number of cases	Percent of all cases	Median loss
Noncash	426	22%	\$66,000
Billing	424	22%	\$100,000
Expense reimbursements	248	13%	\$50,000
Check and payment tampering	217	11%	\$155,000
Cash on hand	205	11%	\$50,000
Skimming	200	10%	\$43,000
Cash larceny	192	10%	\$50,000
Payroll	190	10%	\$50,000
Register disbursements	52	3%	\$50,000

forv/s mazars, LLP. All rights reserved.

FIG. 8 HOW LONG DO DIFFERENT OCCUPATIONAL FRAUD SCHEMES LAST?



rights reserved.

FIG. 58 HOW DO VICTIM ORGANIZATIONS PUNISH FRAUD PERPETRATORS?

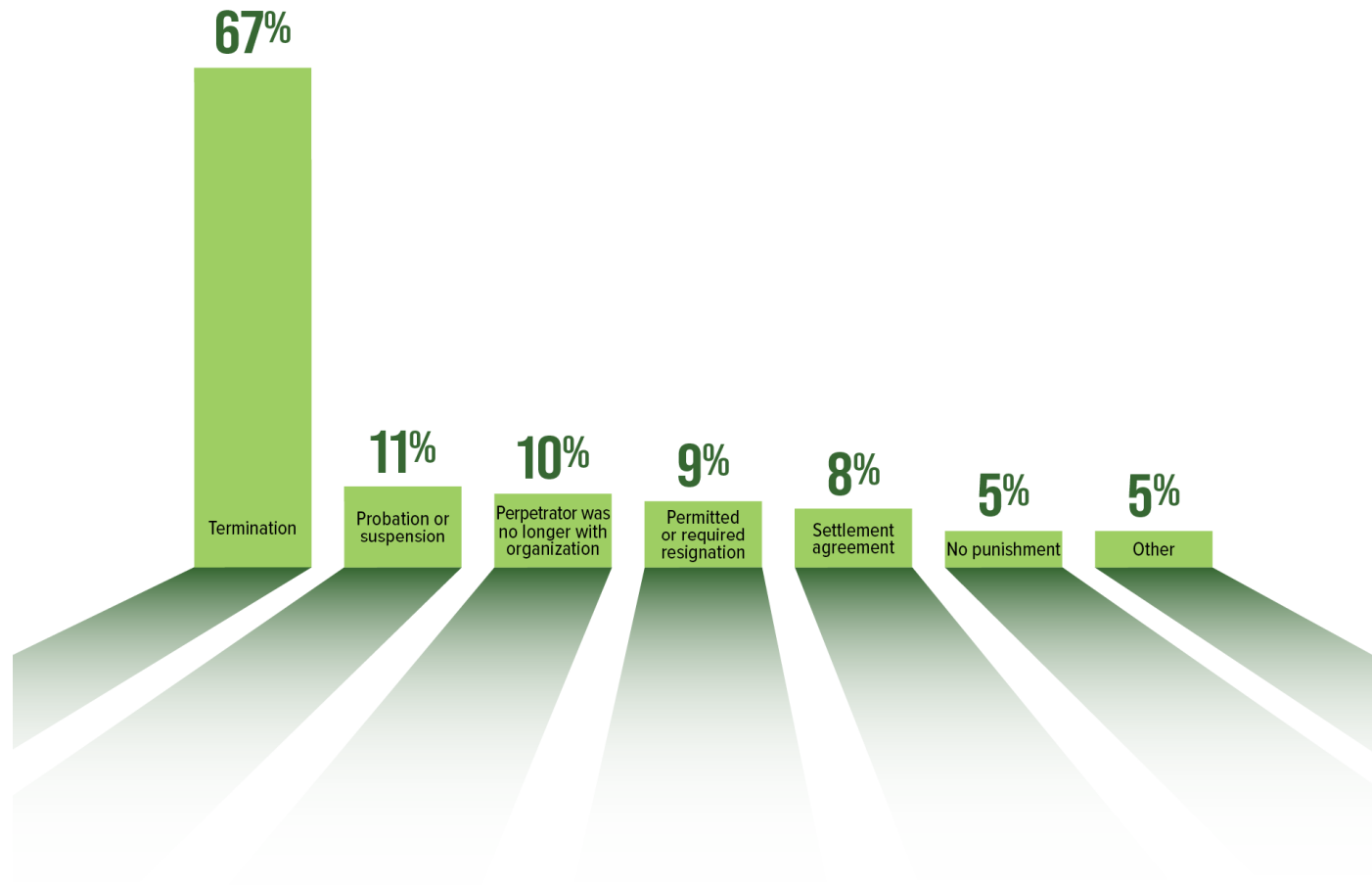


FIG. 10 HOW DO OCCUPATIONAL FRAUDSTERS CONCEAL THEIR SCHEMES?

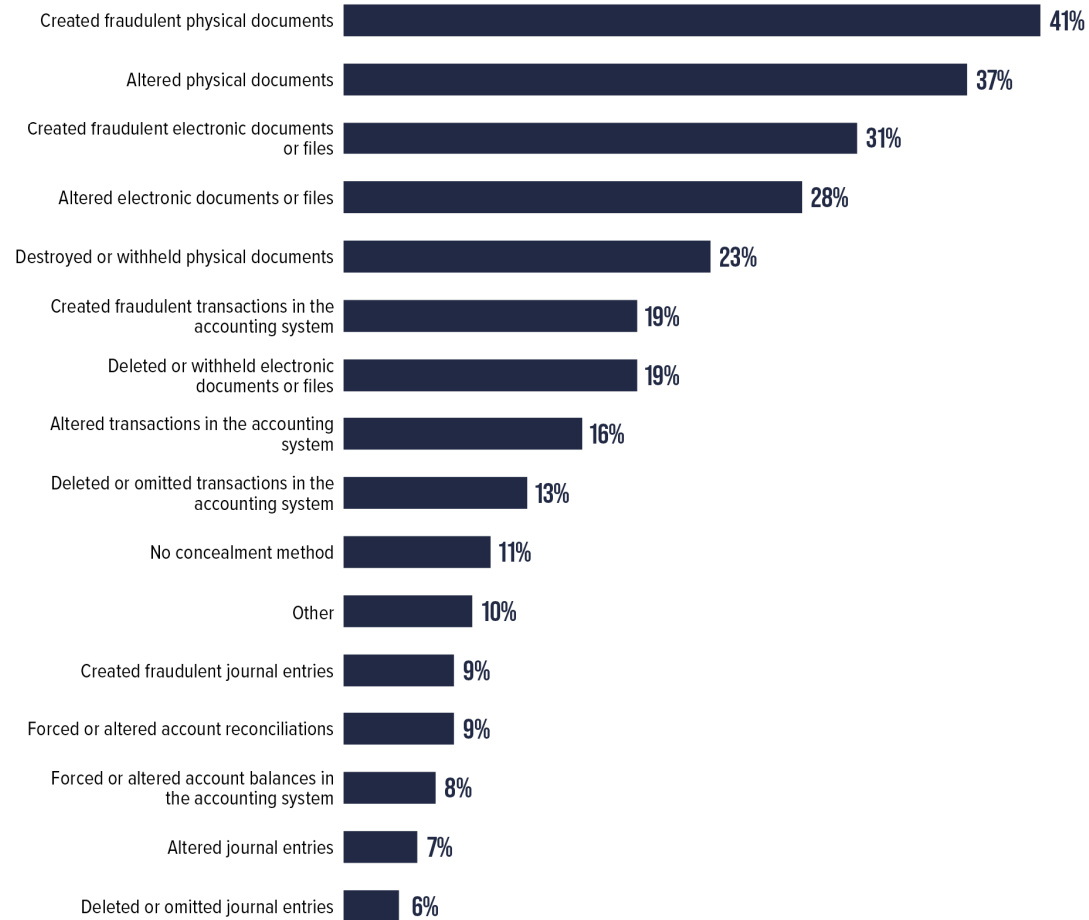


FIG. 13 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

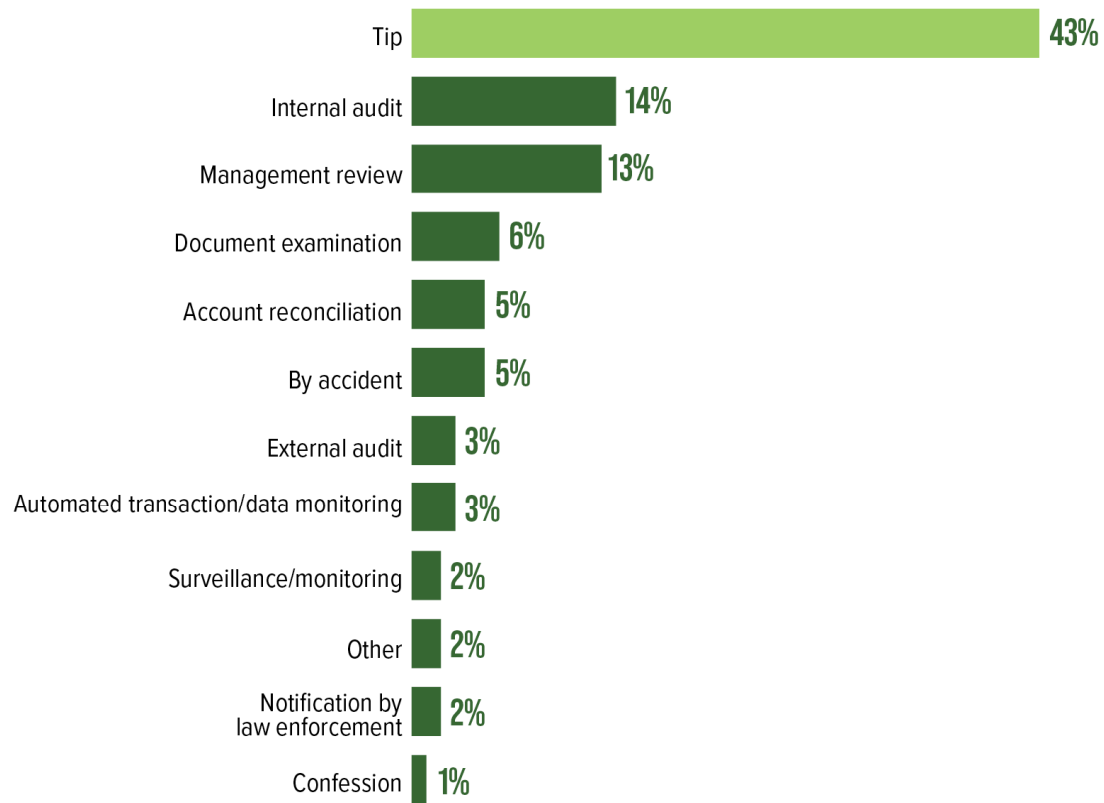


FIG. 38 TOP THREE INTERNAL CONTROL WEAKNESSES BASED ON THE PERPETRATOR'S POSITION

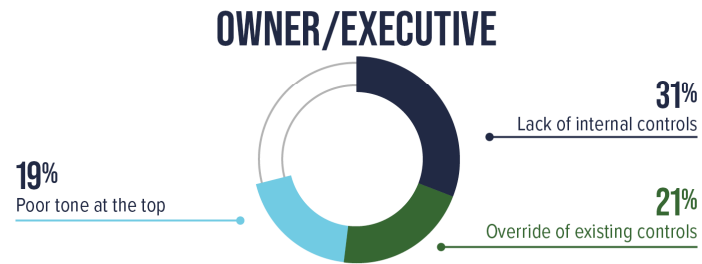
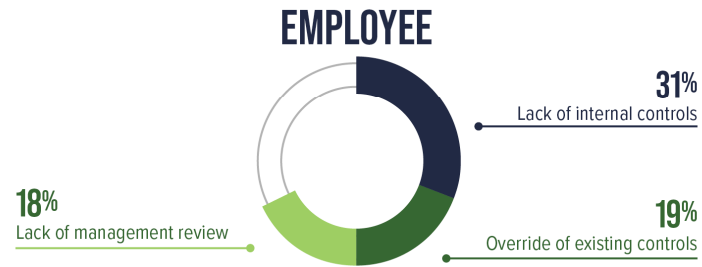


FIG. 47 HOW DO GENDER DISTRIBUTION AND MEDIAN LOSS VARY BASED ON THE PERPETRATOR'S LEVEL OF AUTHORITY?



FIG. 34 WAS A BACKGROUND CHECK RUN ON THE PERPETRATOR PRIOR TO HIRING?

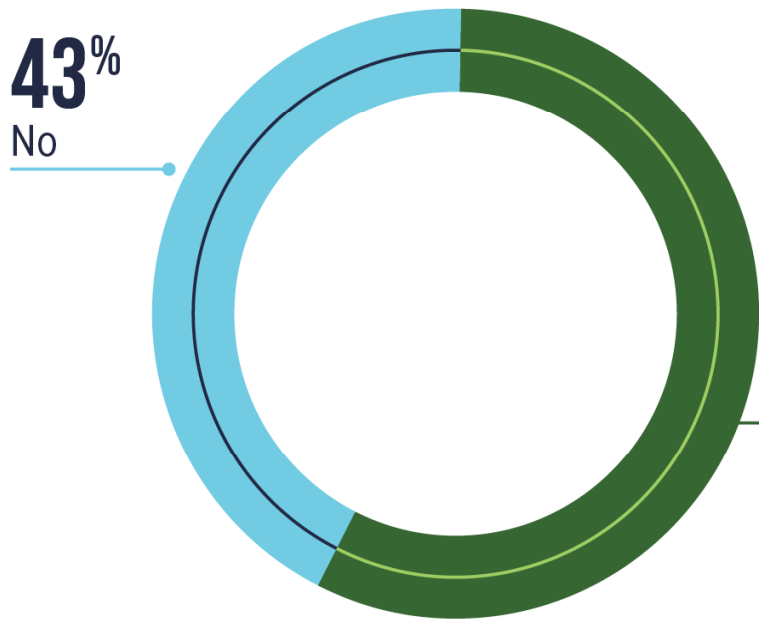


FIG. 35 DID THE BACKGROUND CHECK REVEAL EXISTING RED FLAGS?

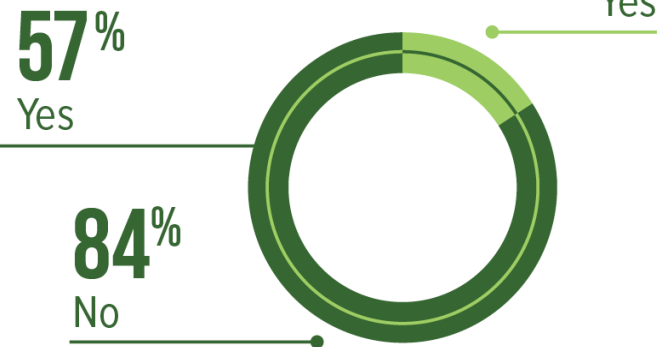


FIG. 58 HOW DO VICTIM ORGANIZATIONS PUNISH FRAUD PERPETRATORS?

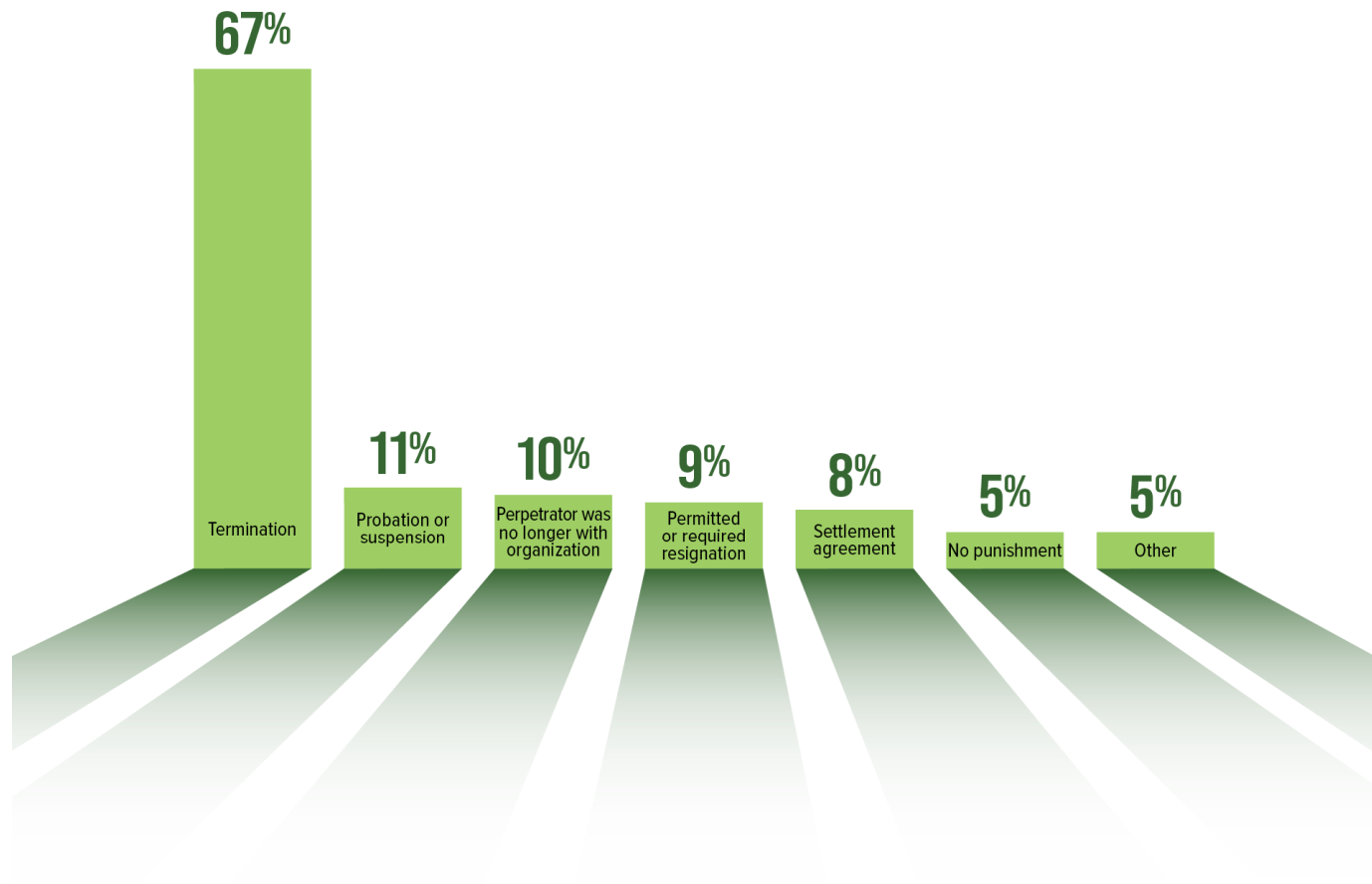
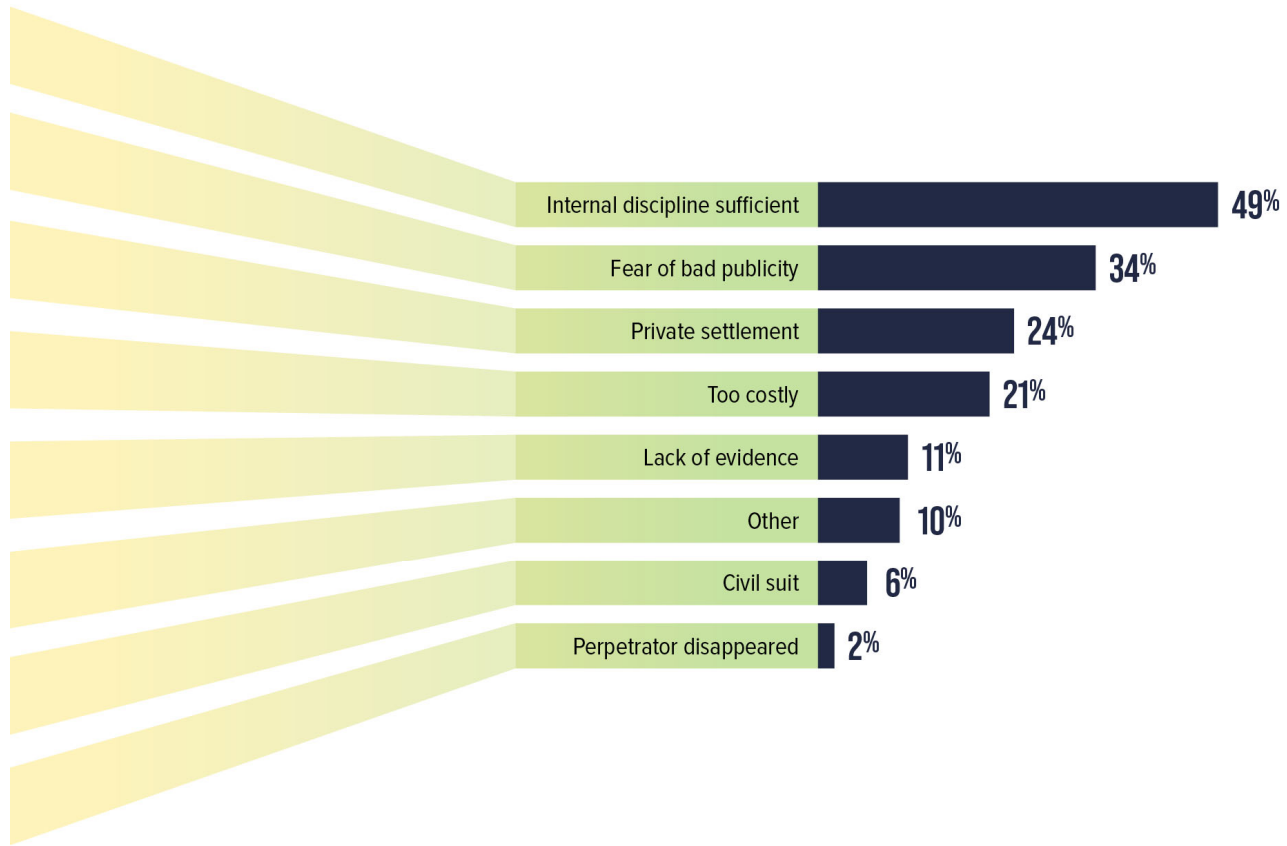


FIG. 59 WHY DO ORGANIZATIONS DECLINE TO REFER CASES TO LAW ENFORCEMENT?



Process vs. Control

Process	Control
Captures data, changes data, & potentially introduces possible errors	Does not change; prevents or detects & corrects errors introduced through processes
Process: post, payment, compile, prepare, etc. Control: agree, match, approve, review, double check, safeguard, authorize	

Three-Step Process to Understand Controls

- What process is used to complete a transaction?
- What could go wrong?
- What controls are in place to prevent errors?



Strong Control Environment

- Management oversight & involvement throughout process
- Preventive controls
- Detective controls



Control Analysis

- What controls are in place?
- Are there any gaps that need to be addressed?
- Do the controls in place provide an effective & efficient organization/operation?



Example Analysis

Cash Receipts		
Process	What Could Go Wrong	Control
Contribution received in mail	Cash stolen	Use of a lockbox, segregation of duties (access, recording & acknowledge letters)
Cash receipts listing prepared	Cash stolen	Use of a lockbox, segregation of duties (access, recording & acknowledge letters)
Money deposited in bank	Cash stolen	Segregation of duties (access & recording), reconciliation between cash receipts listing & bank deposit
Donor contribution entered into CRM sub ledger (salesforce)	Input/processing error, donor restriction incorrect	Segregation of duties (access & recording), supervisor review & approval of entry
Revenue recorded in GL	Input/processing error, account, period, amount, restriction	Reconciliation between contribution detail & GL
Financial statements created	Wrong line item	Management review & budget comparison

Recommendations – Education

■ **Educate**

- Technology is no substitute for employee education
- Educate & re-educate the entire organization, not just IT
- Include the board, executives, & vendors
- Knowledge is power
- Do not discourage false-positive reporting
- Document your security policies in a knowledge database so everyone understands exactly what is going on & why
- Develop & rehearse a robust incident response program

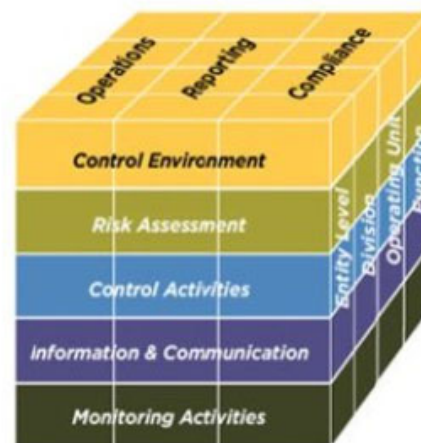


Common Risk Areas



The Control Environment

- Tone at the top – **YES, YOU MAKE THE BIGGEST DIFFERENCE TO PROTECTING YOUR ORGANIZATION**
- Typical management exceptions
- COSO
 - Integrity & ethical values
 - Commitment to competence
 - Board of directors & audit committee
 - Management's philosophy & operating style
 - Organizational structure
 - Assignment of authority & responsibility
 - Human resource policies & procedures



Segregation of Duties

- No single individual is responsible for receiving, recording, & depositing funds or writing & signing checks
- No single individual is permitted to request, authorize, verify, & record expenditures
- Flowchart the process
- In small businesses where fewer people are on staff, consider the power of automation!
 - Accounts payable platforms such as Bill

Categories of Duties

- Custody of assets (access)
- Record transactions (recording)
- Authorization & reconciliation (monitoring)
- Key: Analyze if **access & recording** or **access & monitoring**
- Analyze conflicts & look for potential errors & complementary controls

Example #1

Director of Finance is the only accounting & finance staff

- Access duties – custody of deposits
- Recording duties – all journal entries to record any revenue activity in the accounting system
- Monitoring Duties – all reconciliations (bank, accounts receivable) as well as responsibility for monitoring the classification of revenue

What could go wrong?

What Could Go Wrong?

Director of Finance could remove & keep cash from the deposits & conceal through writing off A/R & adjusting all reconciliations

How to Lower Chance of Error/Fraud

- Since there is no other staff on the accounting/finance team, there are no further segregation of duties
- Complementary controls – All items to be deposited are logged by a staff prior to handing off to the Director of Finance for deposit. Or use a lock box that would funnel deposits through the bank directly
- Compensating controls – Operations team ties deposit slip back to A/R log after funds are deposited, CEO reviews all reconciliations

Example #2

CEO

- Access duties – receive payments
- Recording duties – initiate &/or approve write-off of an uncollectible account
- Monitoring duties – review bank reconciliations prepared by accounting/finance team

What Could Go Wrong?

CEO could receive & keep a payment, then initiate & approve the account write-off.

CEO could also take a payment & not give it to the operations team to include on the A/R log.

How to Lower Chance of Error/Fraud

- Segregate duties to remove the CEO's ability to either accept payments or to initiate/approve account write-offs
- Complementary controls – Write-offs require another signature before processing, the CEO has no access to record write-offs in either the CRM database nor the accounting system. Use a lock box that would funnel deposits through the bank directly
- Compensating controls – Report of all write-offs that occurred in the CRM database in a month are reviewed by the CEO as well as the operations team

Segregation of Duties

- Receipts process
- Payroll process
- Bank reconciliation process
- Expense reimbursements process
- Credit card process
- Outsourcing accounting services
- Use technology & automation
 - For example, vendor analysis tools, payment analytics

Segregation of Duties – Governance

- Officer receive online view-only access
- Examine each check for an unrecognized payee, unusual endorsement, or other indications of irregularities
- Review wire transfers & the bank accounts to which the transfers were made & ask questions
- Debit blocks for ACH with your banker
- Positive pay services

Segregation of Duties – Governance

- Verify payroll names
- Do not allow controller/bookkeeper to sign checks
- Do not sign checks which have not been completely filled in
- Fidelity insurance
- Review supporting documentation closely looking at names, dates, address, EIN, etc.
- Vendor checks
- Vacations, cross-train
- Variance analysis

Controls Over Bank Reconciliations

- Time frame to be completed
 - System access
 - Reconciliation to the general ledger
 - Who does the reconciliation?
 - Approval procedures
 - Bank statements
- Wire transfer procedures
 - Mail handling; random checks
 - Who opens the mail?
 - Monitoring processes

Controls Over Payroll & Hiring Process

- Time sheet approval
- Encourage/require a direct deposit requirement for payroll
- Separate bank account for payroll – zero balancing account
- Use third-party administrator/staffing services
- Background & credit checks
- Exit interviews
- Reference checks – beware of internal referrals
- Past work experience checks

Controls Over Inventory

■ Inventory

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?
- Classification of inventory



Controls Over Disbursements/Contracts

- Set up approved-vendor list
- Invoice approval procedures – delegation of authority
- Petty cash
- Check processing & **don't forget wires**
- Limit employee advances & reimbursements
- Periodic review by an objective person of the list of all vendors receiving fees/checks from the business (a common scheme involves creating a fictitious vendor)

Case Examples

- From a [Washington Post](#) article, a former employee of the Association of American Medical Colleges was able to create fake invoices in the names of legitimate groups that she then approved for payment. When the checks were ready, she had them returned to her, not sent to the vendors. Under that system, a spelling change of just four letters allegedly netted \$3.7 million for her when she purportedly created nearly 200 false invoices in the name of the well-known Brookings Institution policy center, but deposited the checks into accounts she opened for her own “Brookings Institute.” She was later sentenced to 46 months in prison
- A bookkeeper was [sentenced to two years in prison](#) for stealing \$800,000 from National Veterans Service Fund in Connecticut from 2009 to 2014, writing checks to herself & then altering the ledgers to make it appear the money went to veterans

Red Flags for Expense Reimbursement & Credit Card Schemes

- Purchases that do not appear to be business related
- Missing original documents supporting expenses
- Altered receipts
- Many receipts from the same vendor
- Submitted receipts are consecutively numbered
- Expenses in round dollar amounts
- Expenses just below receipt submission threshold
- Segmenting expenses across periods to remain below receipt submission threshold
- Cash payment for expenses typically paid with credit card



Improving Expense Reimbursement Processes

- Review & update reimbursement policies
- Formalize expense reimbursement process
- Review work/vacation schedules
- Institute use of mileage tracking apps



Expense Reimbursement, Credit Cards, P-Card Schemes

- Any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses
- Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc., as incurred business expenses
- Employee purchases personal items & requests reimbursement from the employer



Corporate Credit Cards

Problems in Many Organizations Include

Wasteful & improper spending

Lack of documentation, e.g., receipts, invoices

No explanation of business purpose

Personal charges to be “reimbursed later”

Lack of adequate policies

Expectations not communicated to employees

Lack of second review of all charges

Lack of adequate review of charges by key employee (& any relatives of who also are employees)

Controls Over Credit Card Purchases

- Policies & procedures
 - Employee signature
 - Documented business purpose
 - Number of users
 - Limits
 - Authorization
 - Monitoring
- Review (the right people at the right level)
 - Get supporting documentation for purchases
 - Address possible weakness in the review process
 - Question any potentially inappropriate purchase

Improving Credit Card Processes

Monitor Credit Card Holders & Implement a Two-Step Approval Process

Limit the Use of Personal Credit Cards

Do Not Allow Personal Purchases on Corporate Credit Cards/P-Cards as a Standard Practice

Set Reasonable/Lower Credit Limits

Merchant Code Blocking (P-Cards)

Electronic Analysis of Charges



Controls Over Receipts

- Use a lockbox
- Involve a second person in cash receipts processing
- Verify cash logs
- Make bank deposits daily
- Receiving credit card payments/receipts (PayPal)
- Physical movement of cash (wires)

Controls Over Physical Safeguards

- Limiting access (locking cabinets, doors, etc.)
- **Don't forget controls over collections & inventory**
- Fireproof safes
- Reconcile physical inventory of furniture & equipment
- Physical inventory
- Cameras

Example




- A machine shop manager at a General Hospital was sentenced to a year in prison for stealing more than \$640,000 in parts, by ordering tools & equipment for his own use as well as by selling leftover brass discs to scrap dealers after they were used in radiation treatments

Cyberthreats

- Malware
- Phishing
- Increased remote workforce
- Mobile Threats

- There continues to be targeted ransomware campaigns focused on specific industries like healthcare & government, among others

Best Practices

-  Review & update policies & procedures annually
-  Perform walk-through of controls either annually or on a rotating basis to determine reliability
-  Annual review of user access rights

Disaster Recovery Plan

Things to Review

- Disaster recovery plan
- Crisis manual
- Business continuity plan

Best Practices

- Plan is up to date
- Plan is reviewed at least annually
- Plan addresses all departments
- Staff & board are appropriately trained on plan

Questions?



^v Thank you!

