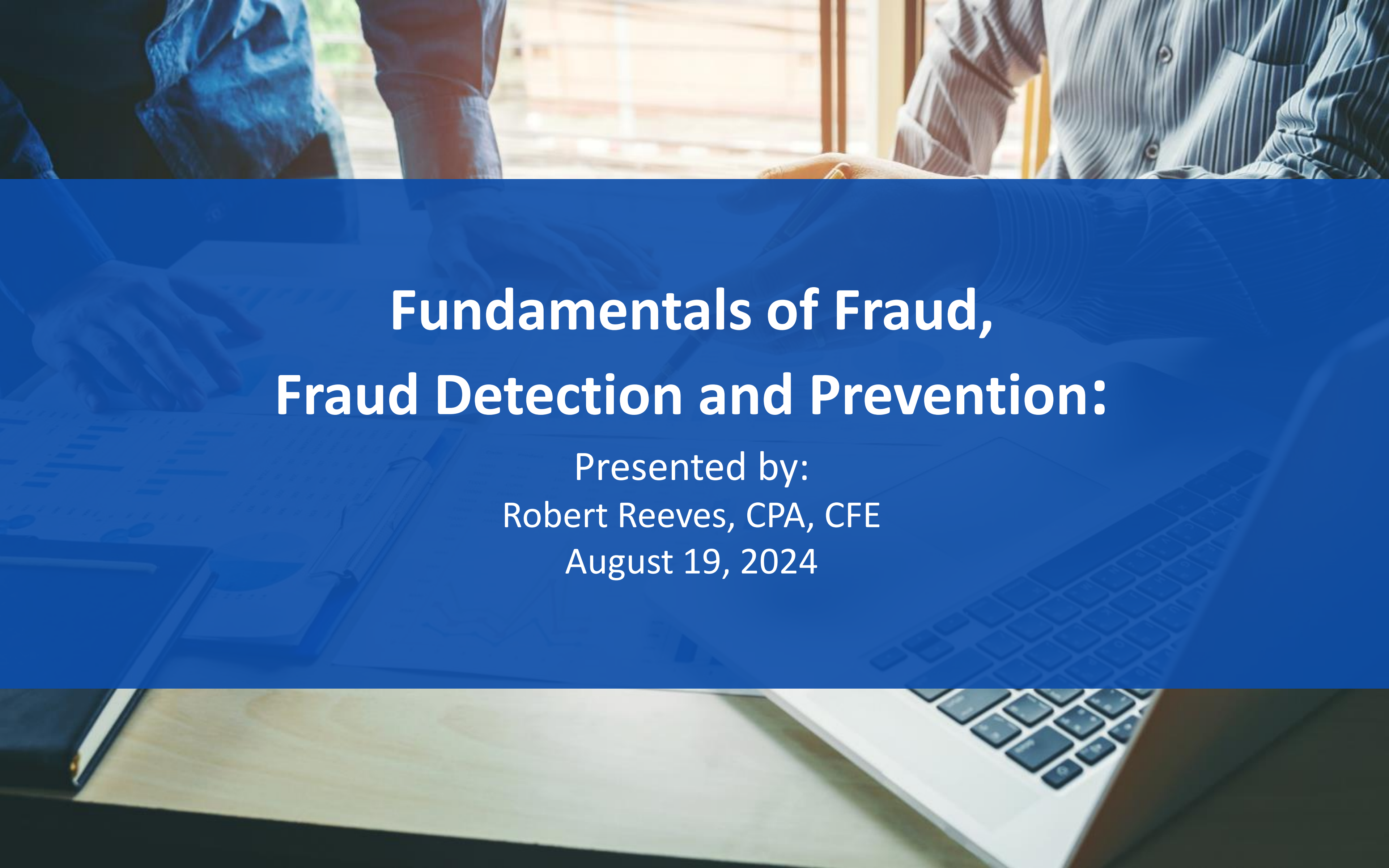
DANNIBLE & MCKEE, LLP

Certified Public Accountants and Consultants

Delivering **Confidence**



Fundamentals of Fraud, Fraud Detection and Prevention:

Presented by:

Robert Reeves, CPA, CFE

August 19, 2024

Fundamentals of Fraud: Fraud Detection & Prevention

Robert Reeves, CPA, CFE

Robert Reeves, CPA, CFE, is an audit partner with over seven years of experience providing audit, review, compilation and consulting services to a variety of clients with a focus in the manufacturing, construction and architectural and engineering industries. Bob also specializes in employee benefit plan audits, forensic accounting services and providing advisory services to clients to help identify and resolve accounting issues. He is the partner in charge of recruiting and client services in the capital region.

Academic and Professional Credentials

- Certified Public Accountant in New York State (CPA)
- Certified Fraud Examiner (CFE)
- Bachelor of Business Administration in Accounting, Magna Cum Laude, Niagara University (2014)
- Masters in Business Administration, State University of New York at Oswego (2016)

Professional Affiliations and Memberships

- American Institute of Certified Public Accountants (AICPA)
- New York State Society of Certified Public Accountants (NYSSCPA)
- Association of Certified Fraud Examiners (ACFE)

What is Fraud?

Reviewing the fundamentals-

- "Fraud" is any activity that relies on deception to achieve some sort of gain
- Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment"

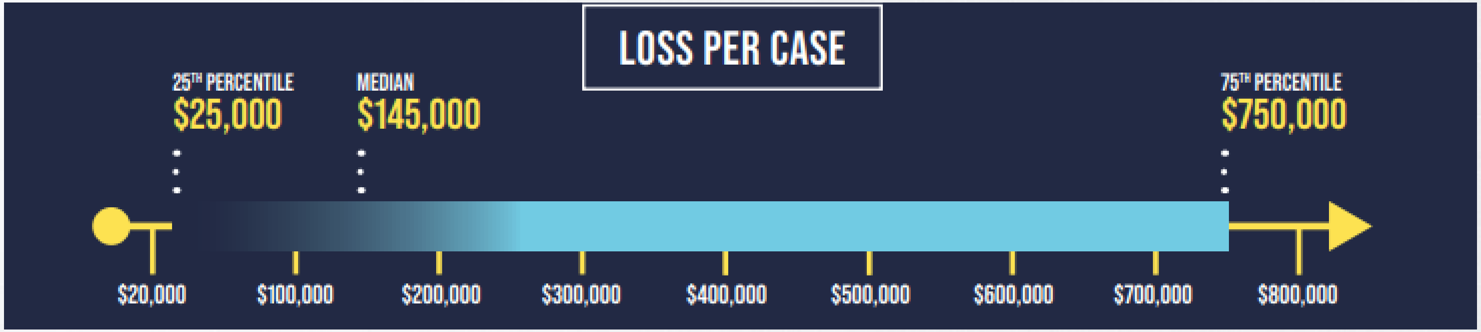
Why are we talking about this?

ACFE's 2024 Report to the Nations

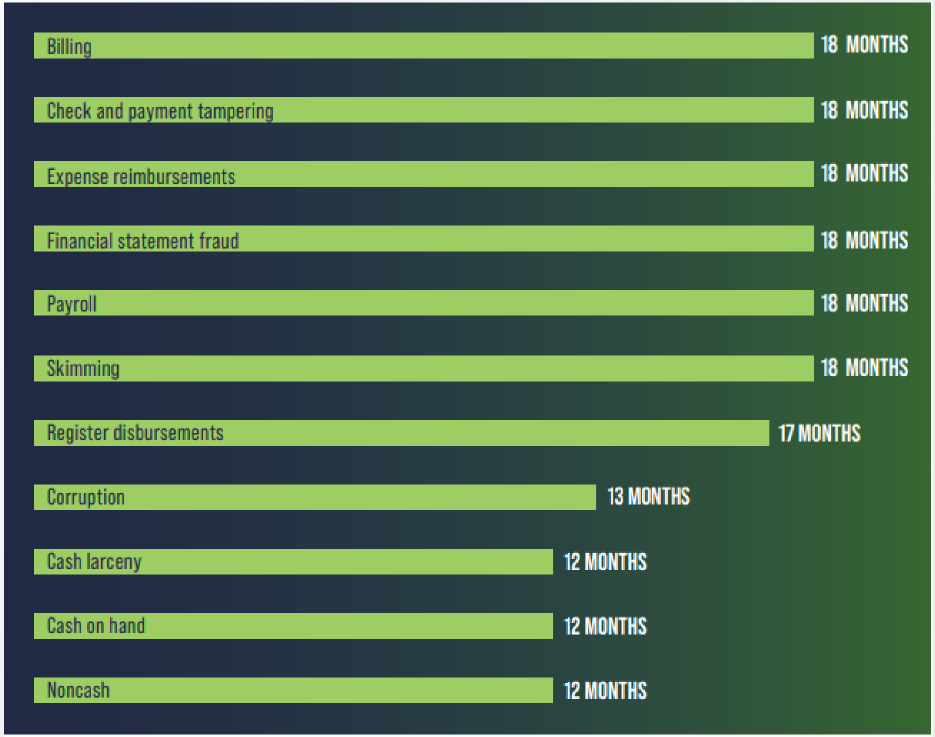
- Case study submitted by CFEs around the world who responded to the ACFE's 2023 Global Fraud Survey
- 2024 report is based on 1,921 cases that collectively cost victim organizations approximately $3.1 billion
- Median loss among the cases in the study was $145,000, up from $117,000 median loss per case from the ACFE's 2022 study
- The 2024 report estimates a typical organization loses 5% of its revenue to fraud each year
- Many frauds go undetected, and many times, organizations don't report the ones they do detect to law enforcement

ACFE's 2024 Report to the Nations

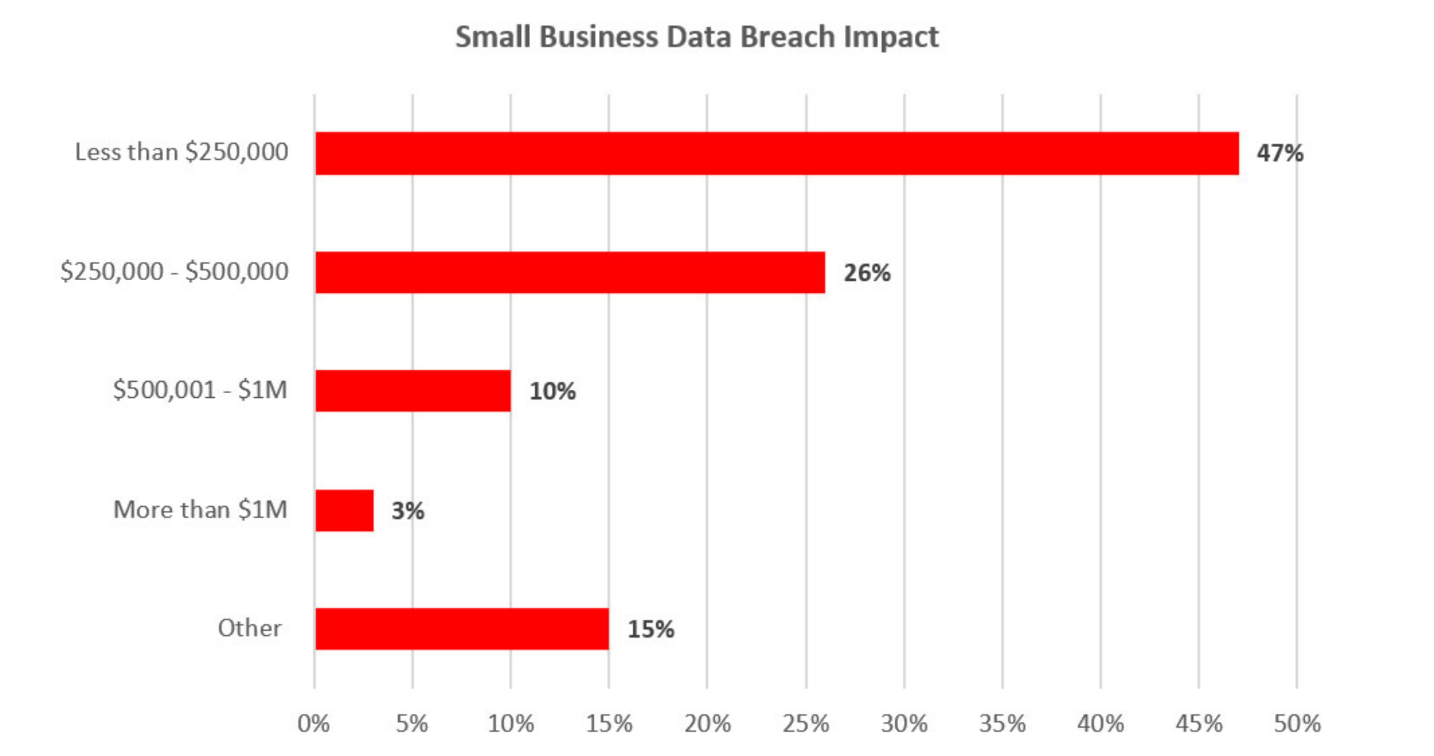
- Fraud is up on average, about 24%
- The study was based on **occupational fraud** – fraud committed by an organization's employees



How Long Do Different Occupational Fraud Schemes Last?



Medium To Small Businesses Are Increasingly Targets of Cyberattacks From Outside Threats



The Final Costs for All Small Business Victims of Data Breaches Included:

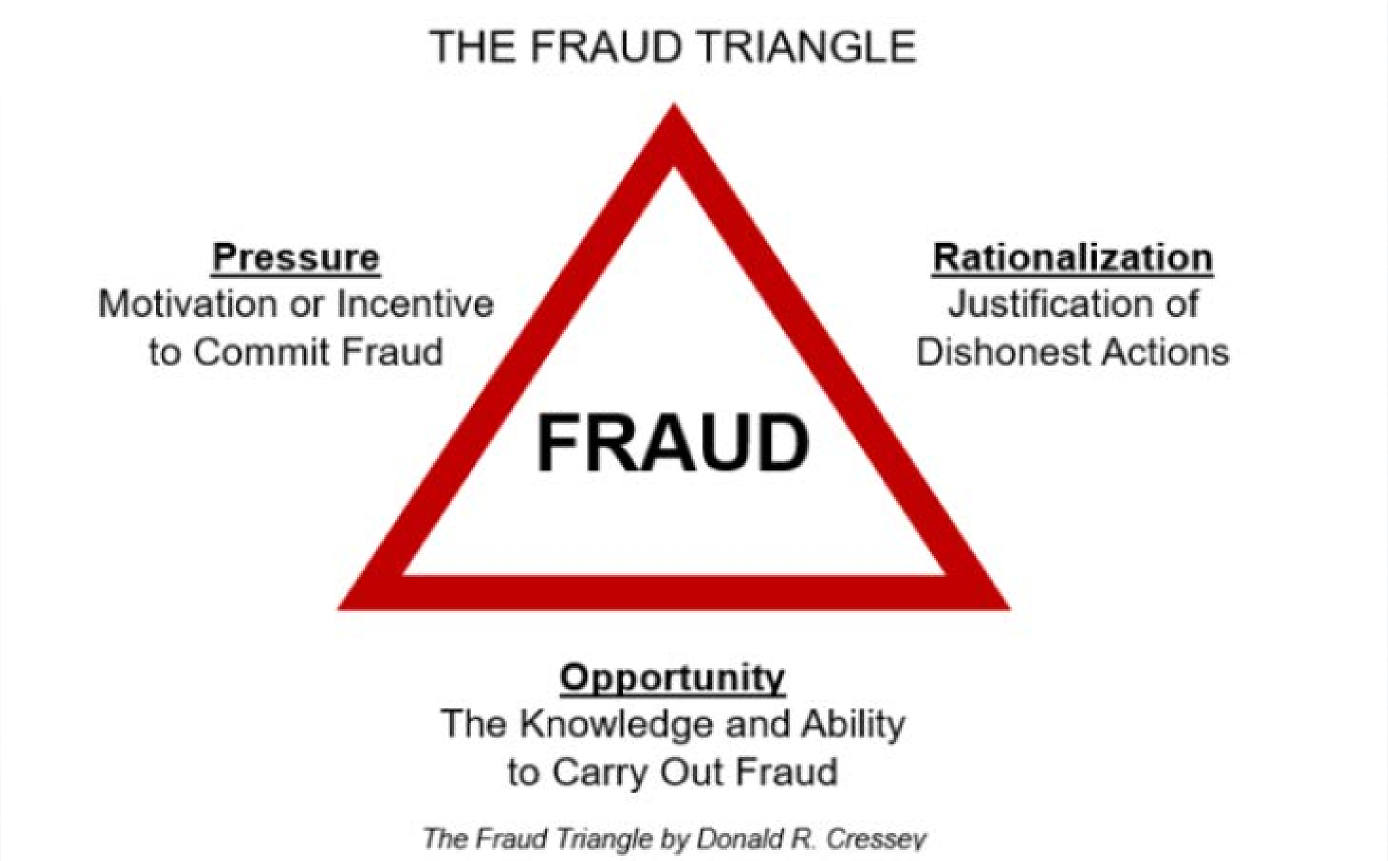
- Lost revenue and customers
- Legal fees
- Fines and penalties
- Insurance coverage
- Security improvements
- Marketing and other business expenses

Impacts of Fraud

- Operational impact
  - If fraud isn't caught it can have a major effect on the operations of a company. It can slow down or freeze operations. Companies have to put a lot of resources towards correcting the aftermath of fraud, when they could have invested in preventing it or mitigating the impact in the first place.

- Customer/reputation impact
  - Fraud can greatly impact the trust that customers have with a company. They will not want to buy from a merchant that they can't trust to protect their privacy and data.

Why do People Commit Fraud?



THE FRAUD TRIANGLE

Pressure
Motivation or Incentive
to Commit Fraud

Rationalization
Justification of
Dishonest Actions

Opportunity
The Knowledge and Ability
to Carry Out Fraud

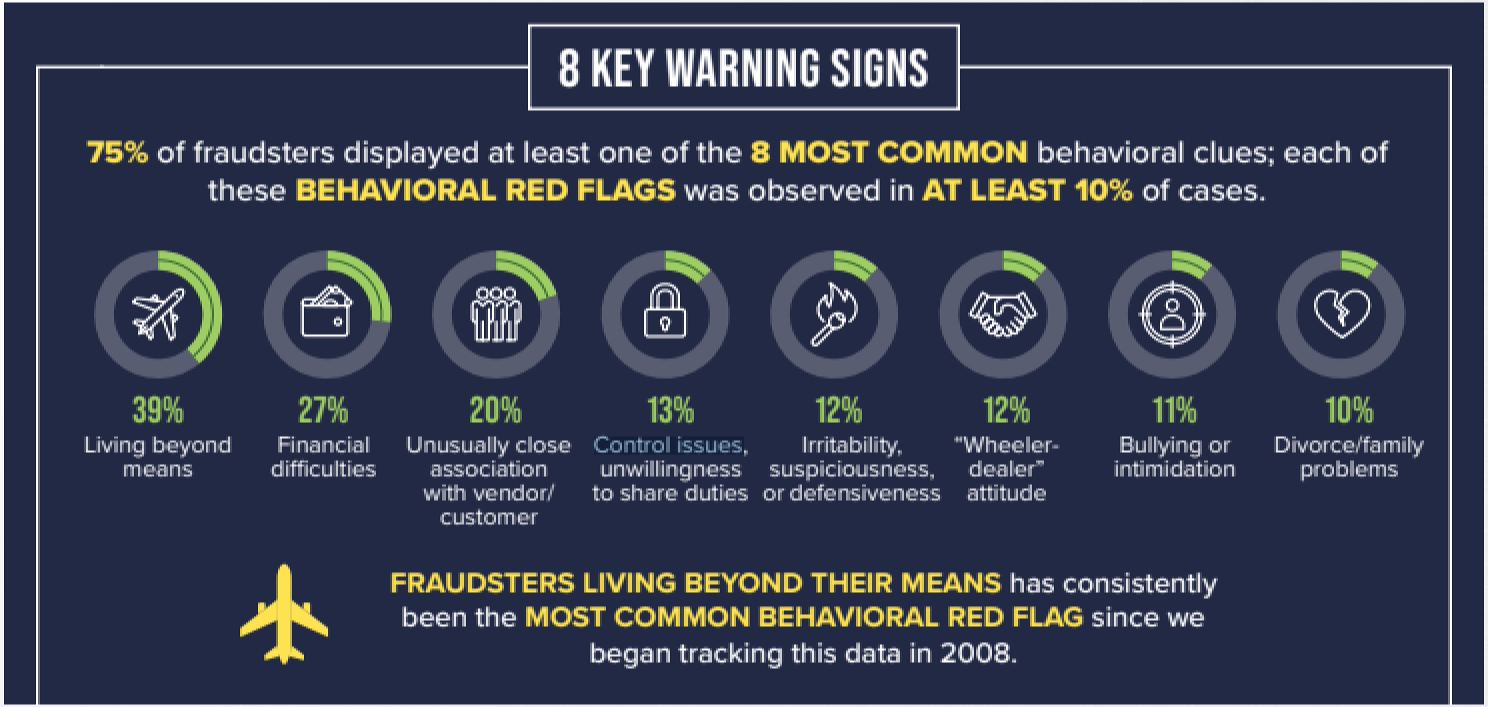
The Fraud Triangle by Donald R. Cressey

Opportunity

- Management that doesn’t promote integrity and honesty
- Weak internal control policies
- Lack of oversight
- Lack of segregation of duties
- Technology and cybersecurity that is not up to date
- Close relationship with a vendor or customer

Motivation

- Employee struggling to make ends meet
- Change in lifestyle (more kids,new house, new car, etc.)
- Addiction
- Living beyond ones means
- They may feel that they need to commit fraud in order to reach their financial expectations (excessive pressure from within the organization)



8 KEY WARNING SIGNS

75% of fraudsters displayed at least one of the **8 MOST COMMON** behavioral clues; each of these **BEHAVIORAL RED FLAGS** was observed in **AT LEAST 10%** of cases.

39% Living beyond means

27% Financial difficulties

20% Unusually close association with vendor/ customer

13% Control issues, unwillingness to share duties

12% Irritability, suspiciousness, or defensiveness

12% "Wheeler-dealer" attitude

11% Bullying or intimidation

10% Divorce/family problems

FRAUDSTERS LIVING BEYOND THEIR MEANS has consistently been the **MOST COMMON BEHAVIORAL RED FLAG** since we began tracking this data in 2008.

Rationalization

- Saving others
- Economic factors
- Job dissatisfaction
- Perceived entitlement
- Creating psychological distance, “there’s no real victim”

Who Commits Fraud?

10-80-10 Rule: supports the general assumption of capability by breakdown of the population and the likelihood of fraud occurrences

- 10% of the population will NEVER commit fraud
- 80% of the population might commit fraud given the right combination of opportunity, pressure and rationalization
- 10% of the population are actively looking at systems and trying to find a way to commit fraud

Who Commits Fraud?

- Well respected people within an organization are 4 times more likely to commit fraud than someone with a lower reputation.
- 70% are within the ages of 36-55
- Fraud is almost twice as likely to occur in groups
- Outside actors of fraud can be many different types
  - Terrorist groups
  - Internet and telephone scammers
  - Person who knows someone in the company or has been wronged by the Company, etc.

Look For Red Flag Data

- Red flag data can teach employees what fraud behavior looks like
- Use the data on behavioral red flags to inform fraud awareness training for staff, managers, and other non-fraud personnel at your organization
- ACFEs 2024 Report to the Nations study found that 43% of occupational frauds were initially detected by a tip

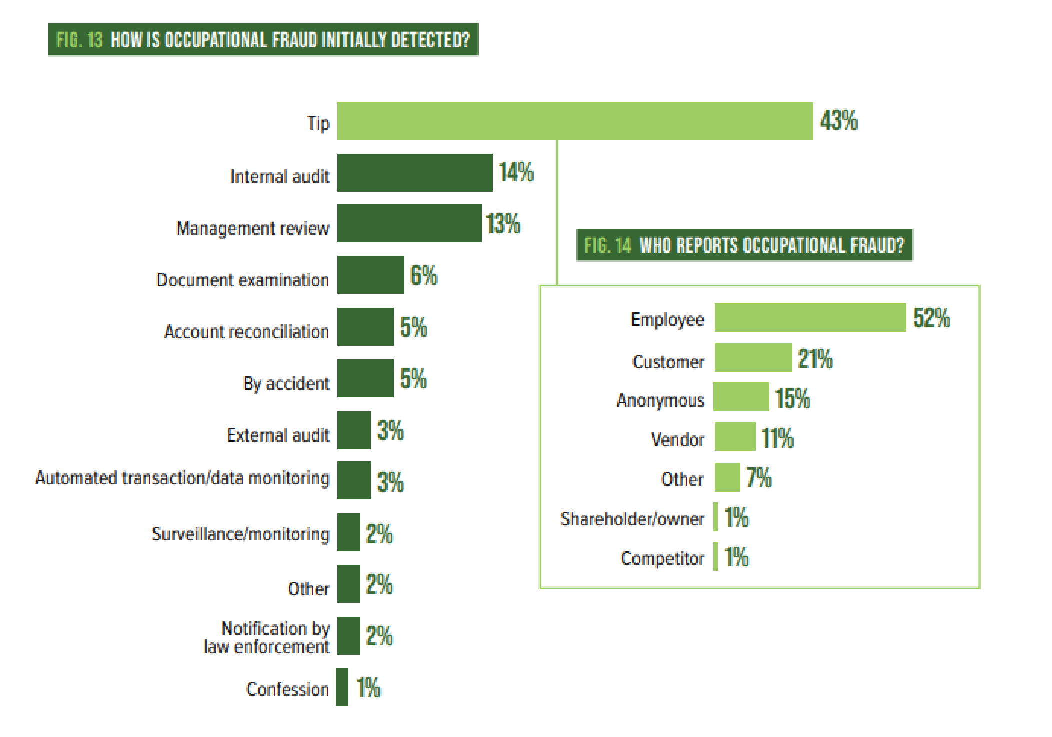


FIG. 13 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

FIG. 14 WHO REPORTS OCCUPATIONAL FRAUD?

The Case of Dixon, Illinois, Comptroller Rita Crundwell

- Rita Crundwell perpetrated one of the largest municipal frauds in history
- She stole almost $54 million over 20+ years in her position as Dixon's comptroller
- Over the course of the 20+ years, the city lacked money to repair streets and sewers and cut back on necessary police and fire department expenditures
- Crundwell owned:
  - 4 properties in Dixon valued at over $3 million
  - Vacation homes in Florida and a ranch in Wisconsin
  - Over 400 champion quarter horses
  - Over $13 million in assets at the time her estate was seized
- Her salary, which was public information, was $80,000 per year

Red Flag Data?!

- Crundwell had unexplainable wealth on a modest (publicly available) salary of $80,000
- The city of Dixon was facing catastrophic budget crises on an annual basis
- The person who handled all the city's money with almost no oversight was living a life wealth and luxury

Could This Have Been Prevented?

- The people who worked for the Dixon city government had never been properly trained to understand the warning signs of fraud
- They had known Crundwell for years and trusted her
- What could have happened if they had been taught the basic tenets of the Fraud Triangle, the importance of controls and the behavioral red flags that tend to occur in fraud cases?
- They might have saved the city millions of dollars had someone raised the attention of the red flags

Lessons Learned

- Rita Crundwell's case is an extreme example, but remember, **tips are the most effective way to catch fraud**, and employee training leads to more tips
- If an accounting clerk who makes $45,000 a year shows up to work one day driving a $200,000 car, its entirely possible that there is a reasonable explanation. But if company records show financial irregularities that could be related to accounts the clerk oversees, the red flag should trigger a heightened level of security.
- Organizations that do not provide fraud awareness training experience median fraud losses two times as much as those that do provide training

Who is Targeted During Fraud?

- Small businesses and consumers are the most targeted during fraud. Small businesses usually have only a few people that look after their internal controls, making them much weaker and vulnerable than larger companies.
- Scammers are also targeting small businesses by impersonating people and companies that you trust. Fake invoices, business impersonation, tech support and fake checks are all scams that scammers target small businesses with.
- It is also reported that private companies and small businesses rank highest in occupational fraud at 42%. The biggest contributing factor is lack of internal controls.

Small Business Fraud

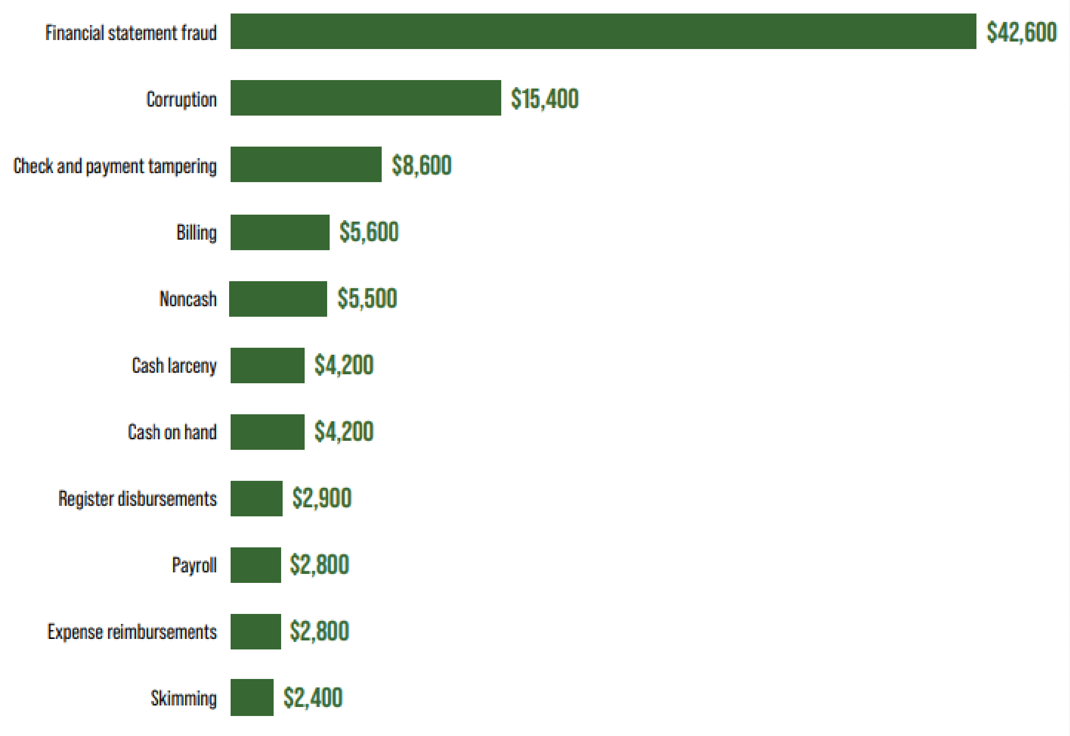
- Small business fraud often occurs within the business.
- Small business fraud has much more of an impact on the business than larger organizations who experience similar business fraud.
- The most common fraudulent areas for small business are:
  - Payroll fraud
  - Cash theft
  - Online banking
  - False invoicing
  - Outside threats (email phishing, etc.)

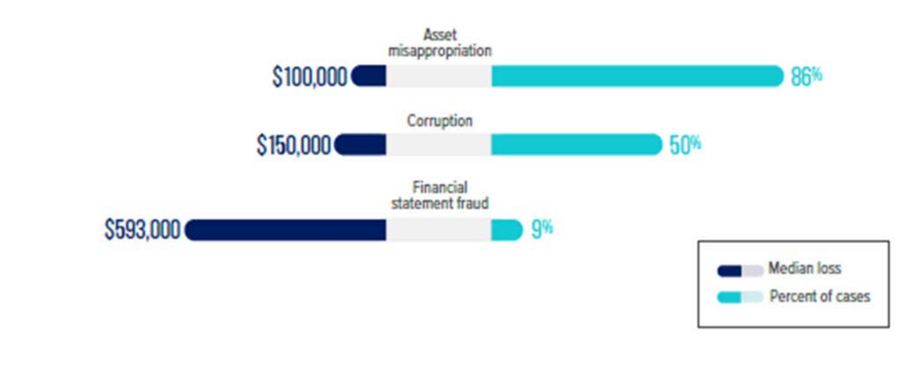
Prevalent Types of Fraud in Small Businesses

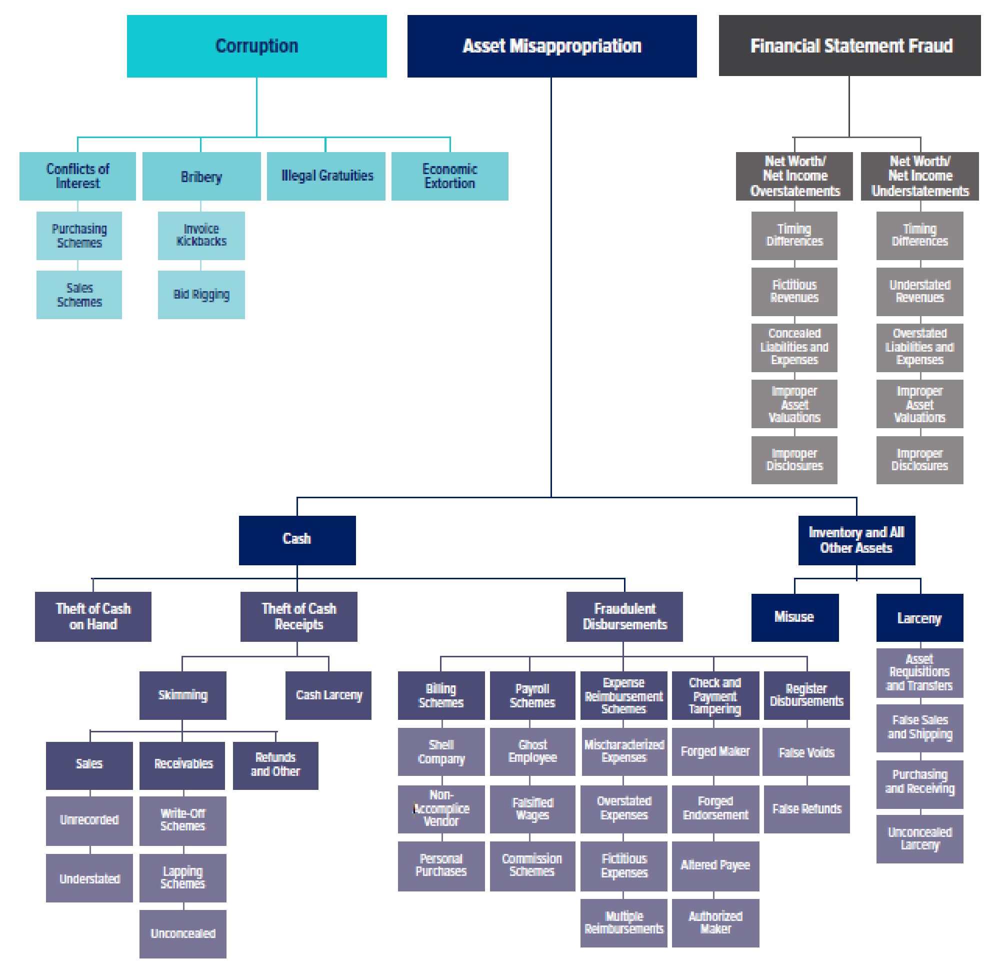
- Misappropriation of assets:
  - Misuse or theft of company resources
    - Expense reimbursements
  - Register disbursements
  - Check tampering
  - Skimming cash

- Financial reporting fraud:
  - Overstating or understating profits, revenue, assets, expenses, etc.

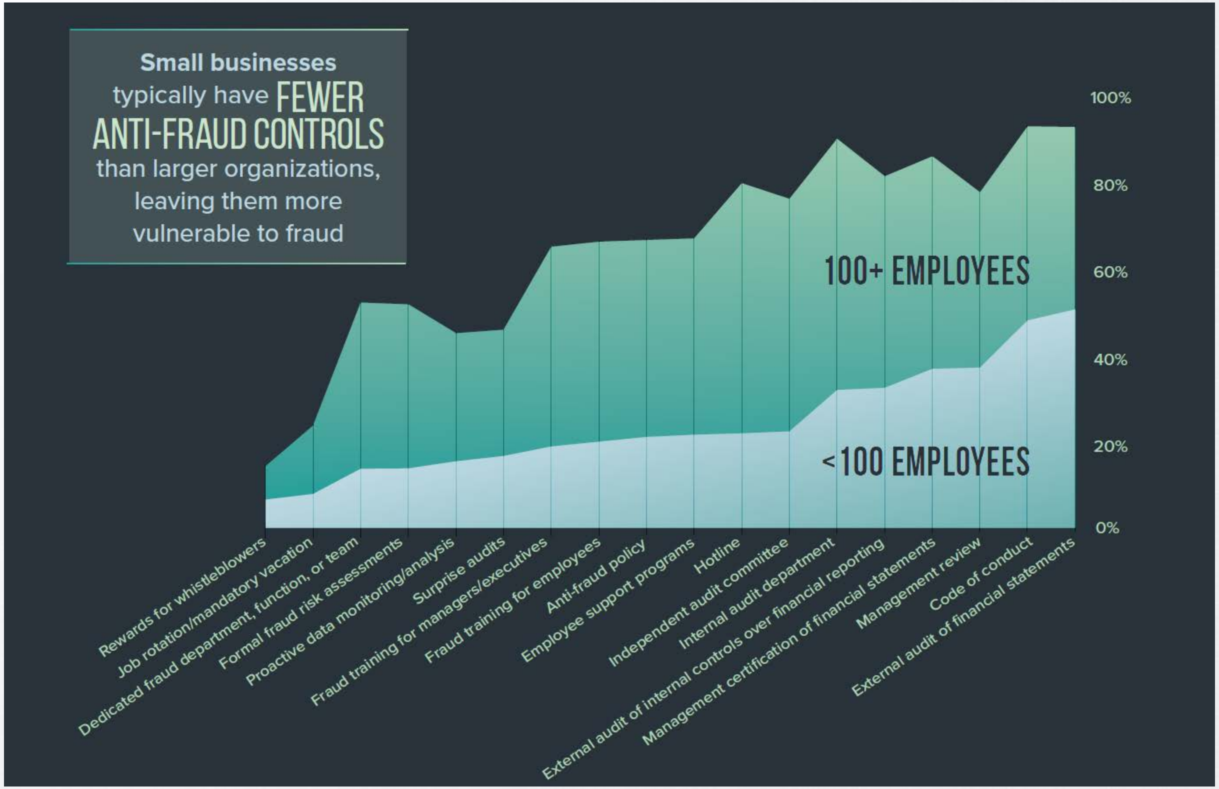
What Is The Typical Median Loss Per Month of Different Occupational Fraud Schemes?




Asset misappropriation
$100,000
86%
Corruption
$150,000
50%
Financial statement fraud
$593,000
9%
Median loss
Percent of cases


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

Small Business Fraud



Small businesses typically have FEWER ANTI-FRAUD CONTROLS than larger organizations, leaving them more vulnerable to fraud

Fraud Prevention and Its Importance

- Fraud prevention is a process that’s aimed to reduce loss in a company and to maintain positive customer service.
- Members of society today value fairness and transparency even more than we had before so it is important to combat fraud which opposes these values.
- According to an ACFE reporting, US businesses will lose an average of 5% of their gross revenues to fraud.

Why is Fraud Prevention Important?

- Every year more and more money is lost to fraud and more reports are made.
- On average, 7,000 reports of fraud are made per day, which really shows the significance of having preventative measures in place.
- It is estimated that 60% of small business losses due to fraud aren't recovered. It is tough for small businesses to stay afloat at times and there are plenty of businesses that wouldn't be able to survive if they were to lose a portion of their revenue due to fraud.

The Most Important Internal Controls for Businesses

Separate Financial Duties

- Many small to medium size business owners and employees are jacks of all trades
  - Quote, negotiate, accept and reconcile payments with customers
  - Calculate and complete deposits
  - Request and approve purchases

- This introduces two risks:
  - Risk of error
  - Risk of theft

Separate Financial Duties

- Dual authorization for purchases/sales over a certain amount
- Different personnel performing check/cash deposits and bank/vendor reconciliations
- Overall review and reconciliation performed by a higher-level personnel not involved directly in day-to-day operational transactions
- Financial controls help managers and owners implement checks and balances
- Ensures all finance are accurate, free from error and protected from misstatement

Regularly Inspect Inventory

- Put control processes in place for inspecting and verifying inventory
- Account for anything lost or stolen
- Verify all orders were accurately fulfilled
- Assign separate employees to sign/approve incoming orders and outgoing orders
- Assign another employee to audit inventory and ensure all records add up

Restrict Access to Financial Systems and Data

- Many employees do not need access to **ALL** systems.
- While it’s important to only give employees the minimum level of access, be even more discerning with financial systems.
- Only give access to those who need that data to do their work, such as your bookkeeper.
- This prevents employees from stealing valuable information or misappropriating funds.

Reconcile Transactions

- Transactions don’t end after you’ve purchased new inventory or sold it to a customer.
- Implement a process to regularly check transactions against your bank accounts — including credit card and cash sales and your own purchases and expenses.
- This ensures that no unauthorized transactions or payments get past you, whether a bad actor got a hold of your card or an employee purchased something they weren’t authorized to.

Randomize Reviews

- Though you should regularly reconcile your transactions and accounts, do so randomly.
- If you keep a consistent schedule, your employees may be able to doctor the books so you don’t see any unauthorized activity.
- Auditing at random dates and times will give you a peek at how your employees handle finances when they don’t know you’re looking.

Monitor Expense Reimbursements

- Employees may use their personal credit card or cash to purchase something for your business.
- Still, you shouldn’t reimburse employees at random.
- Create a process employees must follow to be eligible for reimbursement.
- Commonly, businesses will approve the purchase and the amount and then only reimburse the employee once they provide a receipt.

Additional Controls to Implement

- Compare receipts – confirm receipt match transactions and Pos
- Create a vendor approval process
- Mark all invoices – mark paid invoices to prevent double payment
- Establish a backup record
- Assign two employees to count cash
- Secure blank checks
- Implement expense limits
- Conduct external reviews – seek regular independent reviews

Fraud Detection and Prevention

- Create a zero-tolerance policy for bribery and corruption.
- Check on employees' relationships with clients, especially those in power, periodically.
- Look for suspicious activities like the number of times an employee meets with a client and their location.
- Create an anonymous system to report suspicious activities to the higher power that encourages other employees to report any suspicious activities without repercussion from their boss, manager or co-worker.

Fraud Detection and Prevention

The most important ways to detect and prevent fraud are

- Managing risks
- Strengthening internal controls
- Training your employees
- Enhancing cyber security and conducting audits

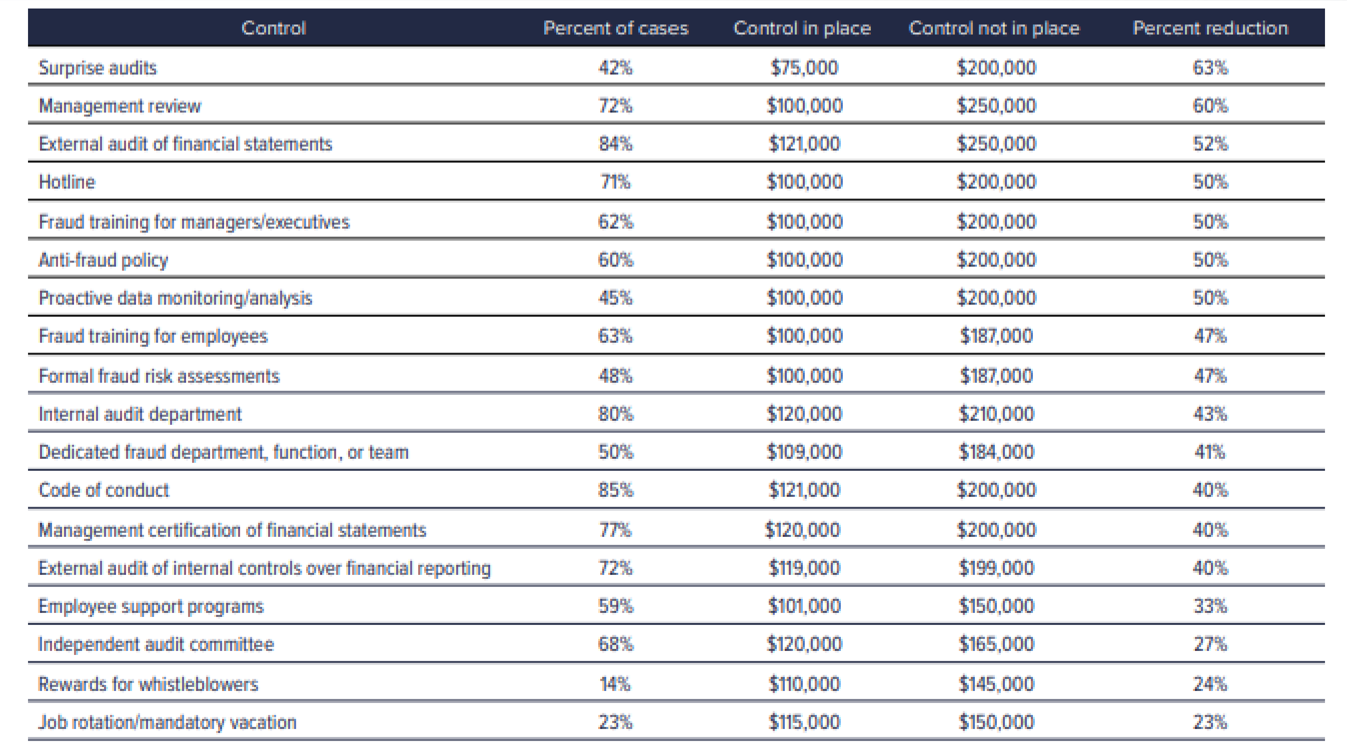
Managing Risks

- It is essential that companies manage risks to respond to potential threats and ensure their assets and reputation are safe.

- It is also important that businesses take a proactive approach when dealing with potential fraud rather than a reactive one.

- Although it might cost money to manage risks and do these things above, businesses will save much more money by doing so then they would lose by remaining vulnerable to fraud.

Impact of Managing Fraud Risks



Control	Percent of cases	Control in place	Control not in place	Percent reduction
Surprise audits	42%	$75,000	$200,000	63%
Management review	72%	$100,000	$250,000	60%
External audit of financial statements	84%	$121,000	$250,000	52%
Hotline	71%	$100,000	$200,000	50%
Fraud training for managers/executives	62%	$100,000	$200,000	50%
Anti-fraud policy	60%	$100,000	$200,000	50%
Proactive data monitoring/analysis	45%	$100,000	$200,000	50%
Fraud training for employees	63%	$100,000	$187,000	47%
Formal fraud risk assessments	48%	$100,000	$187,000	47%
Internal audit department	80%	$120,000	$210,000	43%
Dedicated fraud department, function, or team	50%	$109,000	$184,000	41%
Code of conduct	85%	$121,000	$200,000	40%
Management certification of financial statements	77%	$120,000	$200,000	40%
External audit of internal controls over financial reporting	72%	$119,000	$199,000	40%
Employee support programs	59%	$101,000	$150,000	33%
Independent audit committee	68%	$120,000	$165,000	27%
Rewards for whistleblowers	14%	$110,000	$145,000	24%
Job rotation/mandatory vacation	23%	$115,000	$150,000	23%

Strengthen Internal Controls

- Strengthening internal controls lowers the risk of fraud but also drives efficiency and ensures compliance.
- Create standard operating procedures that properly document the separation of duties at the company and how operational procedures work and periodically audit them.
- Stress the importance of being honest to employees and implement strict access controls, good documentation and technology.

Strengthen Internal Controls

The purpose of strengthening internal controls is mainly being

- To protect assets
- Have accurate records
- Maintain and improve operational efficiency
- Achieve organizations objectives and goals
- Guarantee that policies, rules, regulations and laws are being compiled with

Strengthening internal controls lowers the risk of fraud however it never 100% eliminates it.

Internal Control Standards

- Control environment- establish structure, responsibilities, ethics and a reporting chain.
- Risk assessment- analyze and identify potential risks.
  - Do a brainstorming session with office staff. Ask the questions of what could happen and try and find the exposures
- Information and communication- track information for operations, goals, progress, compliance and create separate lines of communication for confidential information.

Internal Control Standards

- Perform a formal fraud risk assessment and periodically monitor, assess and adjust accordingly based on where the material fraud risks of the Company are

- Operational procedures and internal control procedures need to be evaluated and updated every so often, especially in today's remote environment

Training Your Employees

- It is very important that companies train their employees to be able to recognize possible fraud schemes so that the company is better protected against outside fraud.

- It is also important that a company preaches integrity and honesty to each employee and that the benefits of being honest and having integrity far outweigh the benefits of not.

- Ways to do this include having mandatory training, conducting seminars and promoting culture.

Cyber Fraud in Today's Environment

- Hacking
- Malware
- Identity theft
- Social Engineering
- DDoS attacks
- Phishing scams (smsphishing, video phishing, etc.)
- Password attacks
- Software Piracy

Working at Home Impact on Fraud

- Remote work has increased the risk of confidentiality leaks
- It is much easier for employees or others to steal sensitive data
- Network infrastructure has to be more complex to accommodate remote work
- False “urgent” emails are at an all time high
- Separation of tasks is harder when employees are working apart
- Hard-copy clues that would have helped discover fraud in the past do not exist in the digital age. Organizations should have operational procedures in place that cover tasks being performed remotely.
- Communication between employees generally decreases when they are working from home

‘Boss Scam’ That Targets at Home Workers

- One scam is targeting at home workers by posing as a consumer’s employee and texting and requesting gift cards as work emergency.

- Many New Yorkers have been targeted by this scam as the scam promises to reimburse the employee quickly.

- The text will sometimes include an employee and employers actual name, number and email address making it look legitimate.

- A legitimate employer will never ask you to handle company business through gift card purchases.

AI and Machine Learning

- The ever-advancing technology of AI and machine learning has allowed fraudsters to have more interactions with their victims
- AI is used to replicate voices, images and movements of people
- Fake calls, fake emails, fake video calls where fraudsters are impersonating business executives
- These real-time “deepfakes” present a unique challenge for organizations and individuals
- Scammers continue to use more sophisticated technology and methods to carry out their schemes

Employees 'Faking Work'

- Fake employees are another thing that employers have to worry about when their employees are working from home.
- A dozen Wells Fargo employees were recently fired for allegedly faking work through simulated keyboard activity.
- There are companies that produce software for monitoring employee's presence and in some cases productivity.
- It is important that business owners are aware of this possibility and have checks to make sure they're not getting scammed by their own employees.

Ways to Prevent Fraud : Working at Home

- Remote employees must work on secure networks
- Implement dual factor authentication
- Utilize Firewalls and virus scanners
- Issue company owned devices and discourage employees from working on personal devices
- Making sure that sensitive information is limited and only sent through very secure networks
- Annual security training
- "Trust, but verify"

Enhancing Cyber Security and Conducting Audits

- Having technology that can help prevent attacks and that can root out fraud from outside sources is important especially as you scale your business.

- Audits are also a great way to catch errors and fraud that has material misstatements.

- It is a great idea to hire an independent CPA firm to test and strengthen your internal controls.

Have a Plan

- It is also incredibly important to have a plan for the possibility of fraud being committed.

- Review during your annual insurance renewal what types of coverage you have for employee dishonesty. What insurance do you have for a data breach? Does your insurance cover the cost of legal and forensic work?

- If you have a data breach is there a plan? The company should have a team in place that focuses on what happens. If a data breach were to occur who do employes communicate with? What are the next steps that the company would immediately implement?

Combating Friendly Fraud

- “Friendly Fraud” or refund fraud is on the rise!
- Products are purchased form retailers’ websites and are then deceived into issuing refunds without receiving the product back
- These schemes are often referred to as “Friendly Fraud” because customers’ disputed charges appear legitimate
- These have become a costly and decidedly unfriendly thorn in the side of merchants and financial institutions
- According to the National Retail Federation, retailers lose $25 billion a year to them

Combating Friendly Fraud

- Small, family-owned coffee shop in Quebec, Canada recently lost over $10,000 to customers who ordered two expensive espresso machines
- The customers claimed they did not authorize the purchase of the machines
- The business was able to provide copies of email exchanges supporting the orders
- The credit card companies sided with the customers and the business lost both the money and the machines

Combating Friendly Fraud

- Instances of friendly fraud have surged post-pandemic
- Merchants are doing what they can with limited options
- Many new processing systems collect and maintain transaction data for that can supposedly track analytics in a way to reduce manual hours spent combatting disputed charges between merchants and financial institutions
- Payment system providers are working on improving their systems for communication between merchants and card issuers in the event of a disputed transaction as well

Will These Improved Systems Complicate the Fight?

- Sharing customer data when friendly fraud is identified could run afoul of data privacy rules in certain jurisdictions
- Regulations, designed to protect the consumer, also safeguard fraudsters
- Payment systems' anti-fraud algorithms must distinguish between a real dispute and a fraud where the usual red flags don't apply
- Merchants can alert law enforcement, but it's unlikely resources will be available to protect every illicit chargeback fraud

What You Can do To Protect Yourself From Friendly Fraud

- **Continuous transaction monitoring (CTM)** – these systems monitor financial transactions for anomalies or control violations that might indicate fraud. Without picking samples, software platforms can now analyze billions of transactions related to vendor, customer and employee activities, applying hundreds of targeted tests and algorithms to risk rank them for relevancy – identifying unusual patterns in spending, receivables or disbursements.
- **Data visualization tools**– These can help CFEs, auditors and company personnel understand complex financial data and identify potential risks at a higher level compared to traditional spreadsheets. By presenting information visually, users can flag inconsistencies or areas requiring further investigation and drill down data.

What You Can do To Protect Yourself From Friendly Fraud

- **Artificial intelligence (AI) and machine learning** – training high-risk transactions to "find more like this" with machine leaning is highly effective in identifying potentially improper payments or transactions, and companies are increasingly adopting it for their fraud risk management programs.
- Remember, analytic software is a supportive tool, not a magic cure! Companies will always need strong internal controls and competent professionals such as CFEs.

Balance of Fraud Prevention

- Having a balance with your fraud prevention controls is important

- It is important that you have the right balance of protection and privacy so that customers trust your business but not too much protection that it burdens the customer

- Things like customers transactions getting mistakenly declined can significantly hinder the likelihood they keep doing business with you

Examples of Fraud in New York

Upstate NY Woman Facing Jail Time for Massive Wegmans Wire Fraud

- Long-time Wegmans employee will now serve a prison sentence after it was discovered that she had defrauded the grocery chain out of $568,000.
- Stole over half a million dollars through fraudulent credit card refunds, over 350 transactions.
- Reports claim that she would have pharmacists at the store sign off on what appeared to be legitimate refunds for prescription drugs, then processed the refunded money to her personal credit card.
- In addition, she also stole $11,000 from Wegmans using gift cards.

Upstate NY Woman Facing Jail Time for Massive Wegmans Wire Fraud

- She told the FBI she began stealing funds after her son was born to help pay for medical bills and living expenses.
- She filed bankruptcy in 2014, hoping that would solve her financial instability. It did not.
- In February 2023, she plead guilty, was sentenced to a year in prison and must repay about $580,000 in restitution to Wegmans.

How Could this have been Prevented?

Review and inspection: There should have been reviews and reconciliations of the refunds processed. The amounts the “patients” requested refunds for were fictitious. The orders didn’t exist.

Separation of duties: She should not have been able to request and process the refund. She should have requested the refund and the Pharmacist authorizing it should have then delegated someone else to process the refund back to the “patient.”

Training and Education: There should have been ongoing training on the possibilities of fraud being committed in the Pharmacy department and where the material risks were.

Conclusion

- Fraud prevention and detection only gets more important as your business grows.

- Fraud is a major reason that many business lose money and many fail because of that. It can never be 100% eliminated but your risk can be mitigated by being proactive against it.

- It’s important that all businesses, especially small businesses, invest in ways to prevent and detect fraud.

- The best ways to do this are strengthening internal controls, training employees, enhancing security and auditing.

Questions

Copyright / Disclaimer

This presentation is © 2024 Dannible & McKee, LLP. All rights reserved. No part of this document may be reproduced, transmitted or otherwise distributed in any form or by any means, electronic or mechanical, including by photocopying, facsimile transmission, recording, rekeying, or using any information storage and retrieval system, without written permission from Dannible & McKee, LLP. Any reproduction, transmission or distribution of this form or any material herein is prohibited and is in violation of U.S. law. Dannible & McKee, LLP expressly disclaims any liability in connection with the use of this presentation or its contents by any third party.

This presentation and any related materials are designed to provide accurate information in regard to the subject matter covered, and are provided solely as a teaching tool, with the understanding that neither the instructor, author, publisher, nor any other individual involved in its distribution is engaged in rendering legal, accounting, or other professional advice and assumes no liability in connection with its use. Because regulations, laws, and other professional guidance are constantly changing, a professional should be consulted if you require legal or other expert advice.

Circular 230

Any tax advice contained herein was not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code or applicable state or local tax law provisions.