DANNIBLE & MCKEE, LLP

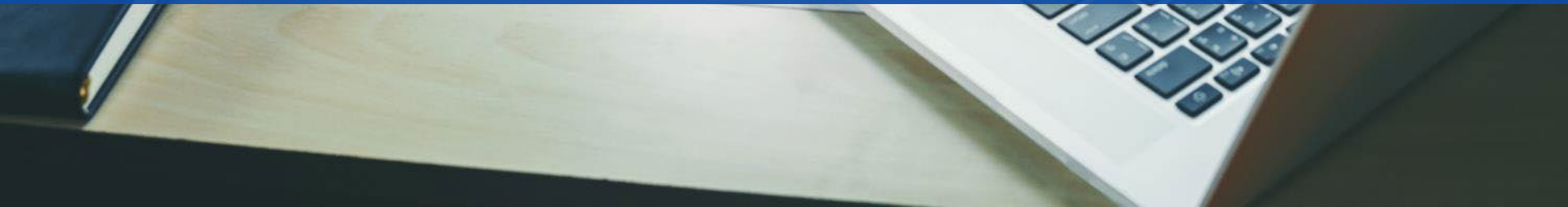
Certified Public Accountants and Consultants

Delivering **Confidence**

What Does Fraud Look Like in A/E Firms?

Presented by:
Kaitlyn H. Axenfeld, CPA/CFF, CFE

November 21, 2024



Kaitlyn H. Axenfeld, CPA/CFF, CFE
Audit Partner

Email: kaxenfeld@dmcpas.com

Web: www.dmcpas.com

Address:

DM Financial Plaza
221 S. Warren St.
Syracuse, New York 13202-1628

Phone: (315) 472-9127, ext. 207

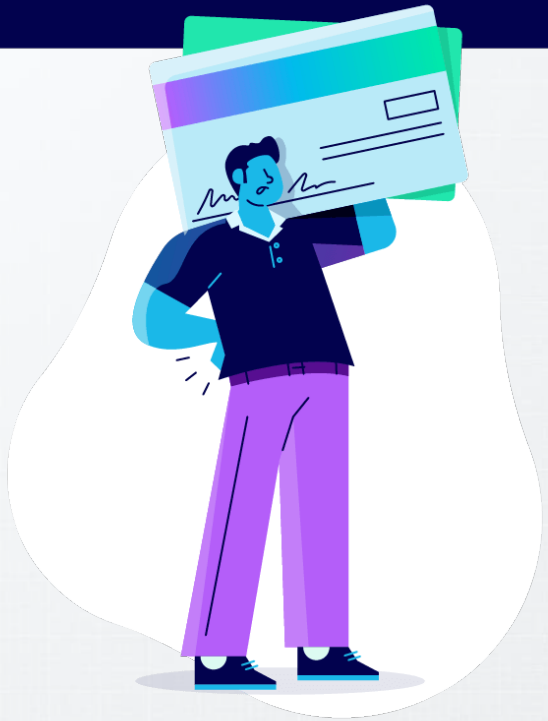
ACFE's 2024 Report to the Nations

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

Why do People Commit Fraud?

Motivation:

incentive or pressure to commit fraud.



Some motivations to commit fraud include:

- Sudden overwhelming expenses, like medical bills or a debilitating addiction
- An unexpected dip in income, like a spouse losing a job
- Frustration with current job expectations or pay

Opportunity:

a chance to commit fraud without being caught.

Opportunities for fraud can occur wherever oversight is:

- Absent
- Unenforced
- Ineffective
- Unmonitored

Rationalization:
reasoning used to justify the fraud.

Rationalizations for fraud include statements like:

- "Everyone skims a little off the top."
- "They expect you to do this—it's one of the perks of the job."
- "We waste so much anyway; why shouldn't I benefit from it?"
- "Our company is so huge, what I'm taking won't be missed."

Who Commits Fraud?

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

According to the "10-80-10 Rule," you can assume that:

10% of people will never commit fraud no matter the circumstances

80% of people might commit fraud given the right combination of pressure, opportunity, and rationalization

10% of people are actively looking for opportunities to commit fraud

Source: *National Association of State Auditors, Comptrollers and Treasurers (NASACT)*

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.

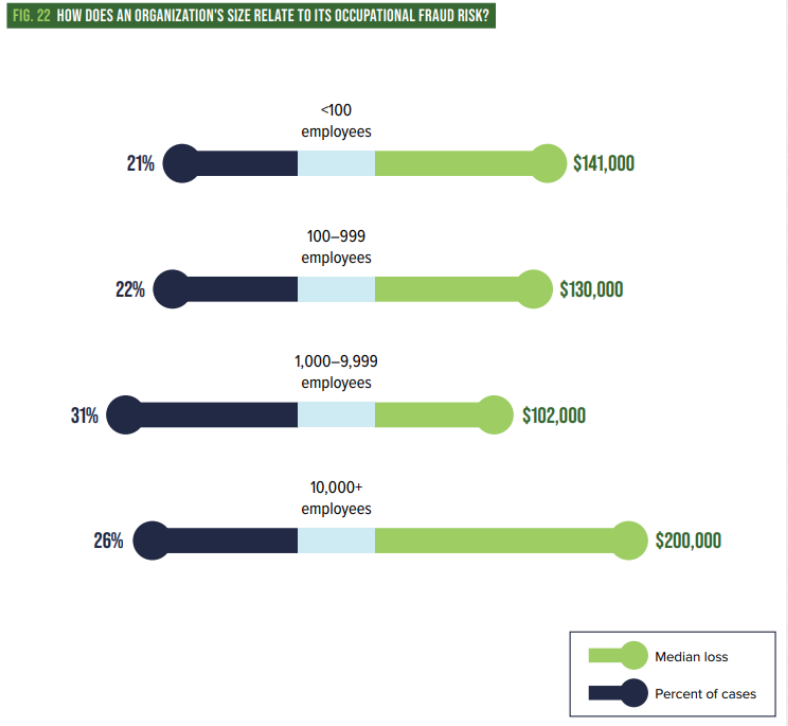
Fraud and the Architecture and Engineering Industry

- Occupational fraud
  - Asset misappropriation
- Cyber fraud

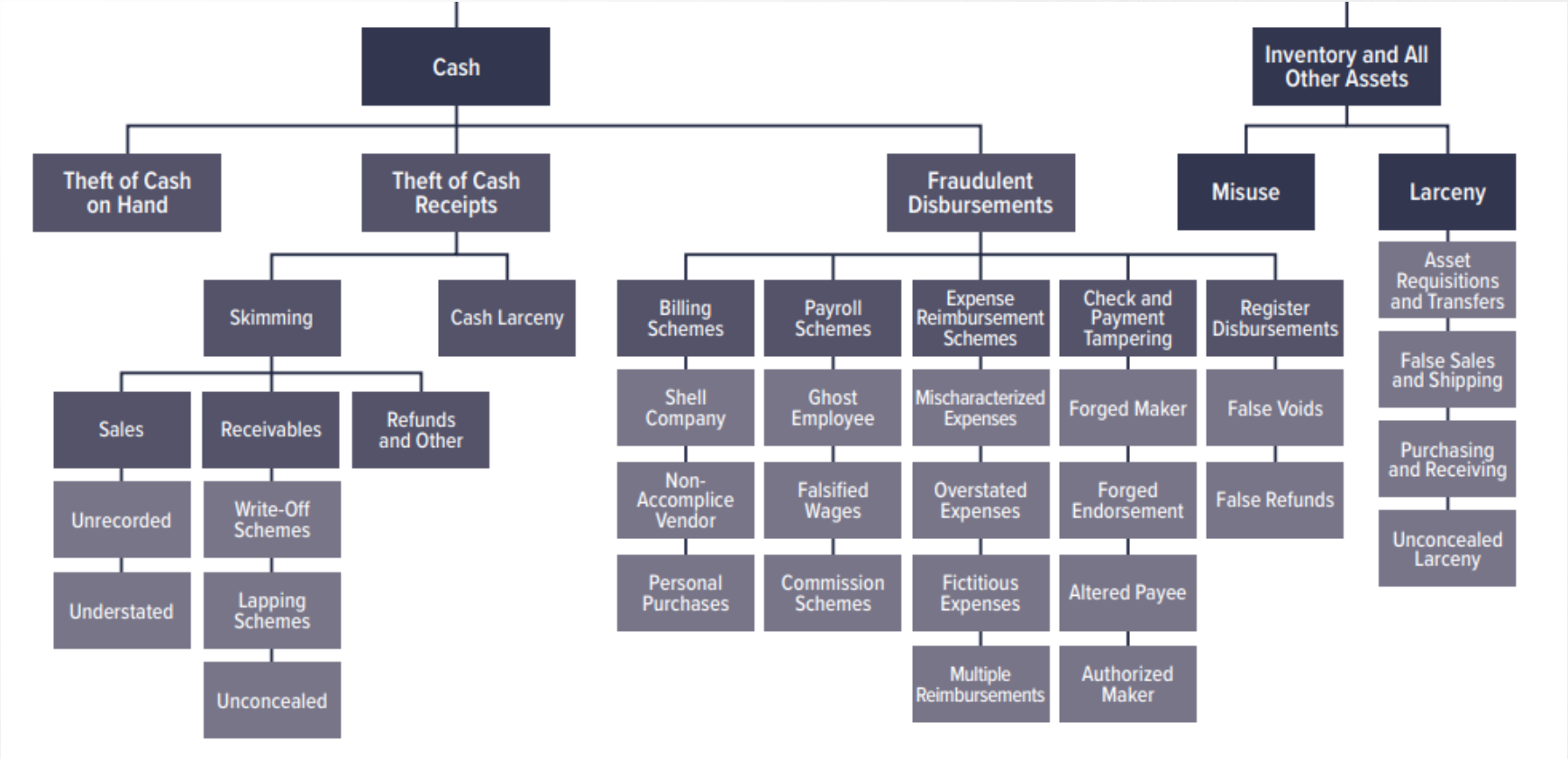
Occupational Fraud is a Significant Threat to Small Businesses

Occupational fraud is a significant threat to small businesses

The smallest organizations suffered the largest amount of fraud cases. These organizations typically employ fewer anti-fraud controls than their larger counterparts, which increases their vulnerability to fraud.



Asset Misappropriation



Asset Misappropriation

Cash

- Theft of Cash on Hand
- Theft of Cash Receipts
  - Skimming, Cash Larceny
- Fraudulent Disbursements
  - Billing Schemes, Payroll Schemes, Expense Reimbursement Schemes, Check Tampering, Register Disbursements

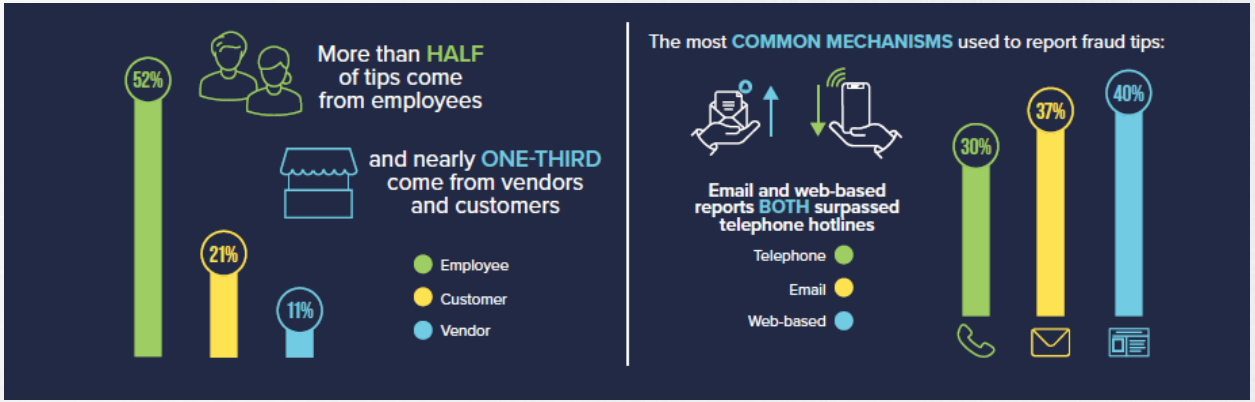
Expense Reports

- Receipt Documentation
- Original Receipts
- Credit Card Policies

Detection – How Do We Detect Occupational Fraud?

Occupational fraud is more likely to be detected by a tip than by any other method.

- The majority of tips reporting fraud come from employees of the victim organization.
- Tips are the most common detection method. Over 40 percent of all cases were detected by a tip.



Managing Third-Party Fraud Risks

All external parties that conduct legitimate business with an organization can pose unintentional fraud risks to the organization.

Types of Third-Party Fraud Risk:

- Legal Risk
- Ethical Risk
- Financial Risk
- Cyber Risk

Managing Third-Party Fraud Risks

Cyber Risk

A weak cybersecurity posture:

- Can make log-in and password credentials visible or easy to acquire;
- Creates a gateway for fraudsters to damage your systems via third-party system connectivity and access;
- Gives fraudsters visibility to your proprietary and confidential information that resides on the third-party system; and
- Enables fraudsters to more effectively create socially engineered phishing, smishing, and vishing communications, increasing the likelihood of success.

Cyber Fraud in Today's Environment

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

Definitions

- **Cyber Crime** – criminal activities carried out by means of computers or internet
- **Cyber Extorsion** - a nefarious cybercrime where threat actors exploit security vulnerabilities to breach digital security systems and gain unauthorized access to valuable assets. These assets range from confidential data and intellectual property to financial currency and critical infrastructure systems.
- **Social Engineering** - The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes
- **Malware** - Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system
- **Ransomware** – Software designed to block access to a computer system until a sum of money is paid

Know Your Scams

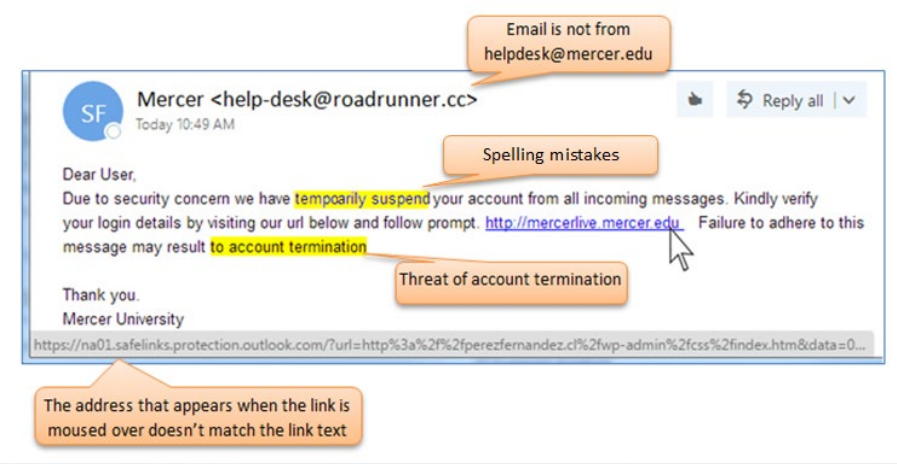
Each of these scams is carried out with the goal of tricking the victim into providing information or clicking on a link, which will install malware onto their device.

- Phishing – carried out via email
- Vishing – carried out via phone
- Smishing – carried out via text or social media
- Spear phishing – targeting phishing in which the fraudster takes time to learn about the victim
- Whaling – targeting executives or presidents with the hope for a bigger return on the phishing investment

Know Your Scams

Phishing - the practice of using deception to get you to reveal personal, sensitive or confidential information

- Spoofed emails and websites



Always:

- Review the greeting
- Look closely at the header
- What is the sender's email address
- Never click on links that are included in email messages

Know Your Scams

Vishing - scam carried out via phone

- spoofing a legitimate phone number
- uses internet phone services (VoIP) to complete the scam
- Combination of 'voice and 'phishing'

Always:

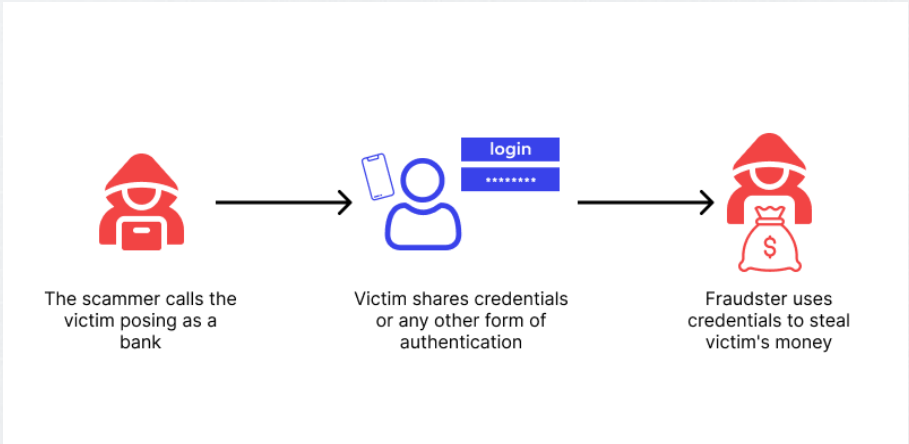
- Be aware
- Don't give into pressure
- Don't answer phone calls from unknown numbers
- Stay calm
- Be skeptical

One form targets your bank account or credit card account:

– *Your account has been compromised. Please call this number to reset your password.*

Other vishing scams include things like:

- Unsolicited offers for credit and loans
- Exaggerated investment opportunities
- Charitable requests for urgent causes
- Extended car warranty scams



Know Your Scams

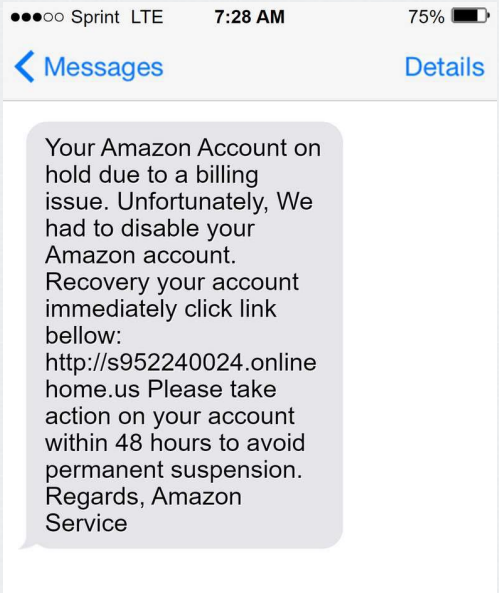
Smishing - scam carried out via text or social media

Combination of 'SMS' (Short Message Services) and 'phishing'

- **Banking Scams:** *"Dear [Bank Name] customer, we've detected unusual activity on your account. Please click the link to verify your transactions: [malicious link]."*
- **Parcel Delivery Scams:** *"Hello, this is [Courier Service]. We've attempted to deliver your package today but failed. Schedule your redelivery here: [malicious link]."*
- **Account Verification Scams:** *"We detected a login attempt from an unfamiliar location. If this wasn't you, please secure your account here: [malicious link]."*
- **Contest Winner Scams:** *"You're the lucky winner of our grand prize! Register here to receive your reward: [malicious link]."*
- **Emergency Scams:** *"A family member of yours has been in an accident. Call this premium rate number for details: [malicious phone number]."*

Best Practices:

- Never click on suspicious links
- Verify independently
- Use phone security features
- Stay updated
- Don't share personal information
- Check for official communications



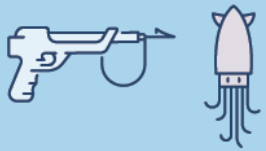
Know your Scams

Phishing vs. spear phishing vs. whaling

Whaling is a specific type of spear phishing, and spear phishing is a specific type of phishing. Learn the differences below.

Phishing
A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

Spear phishing
A type of phishing that targets individuals.



Whaling
A form of spear phishing that targets high-ranking victims within a company.

Know Your Scams

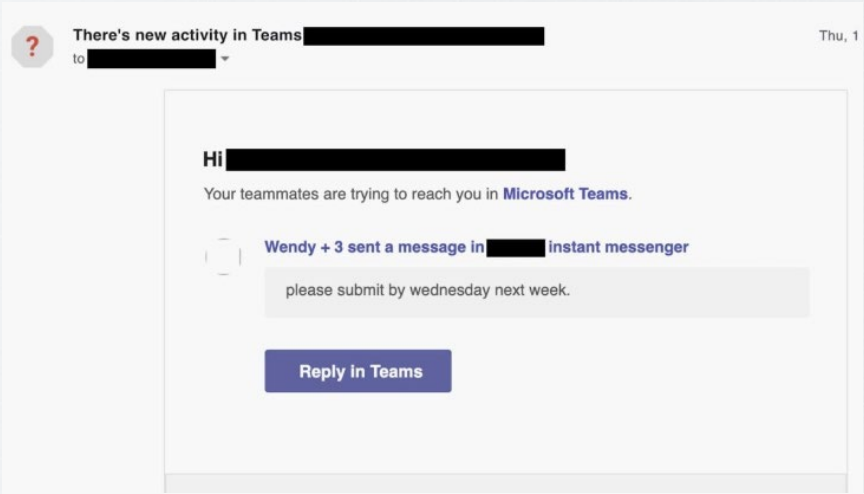
Spear Phishing - targeted phishing, in which the fraudster takes time to learn about the victim.

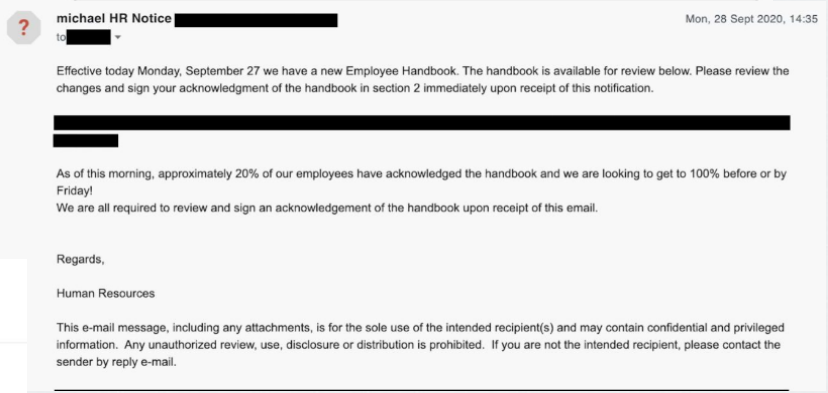
Personalized emails to particular individuals or groups of people with something in common.

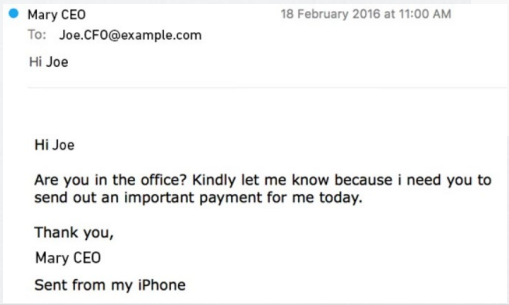
Sole purpose is to get inside the recipient's head and make them think the messages they're responding to are 100 percent legitimate—achieved due to personal touches designed to make them think what they're dealing with is the real deal.

Prevention:

- Two-Factor Authentication
- Password management policies
- Educational Campaigns







Know Your Scams

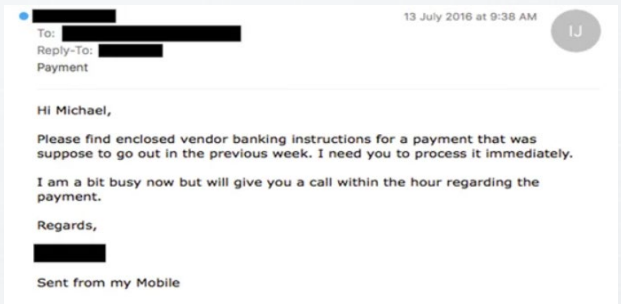
Whaling - targeting executives or presidents with the hope for a bigger return on the phishing investment.

Whaling phishing emails often consist of:

- A sense of urgency
- Personalized information about the target and/or organization
- Corporate/business tone of voice and jargon

Best Practices:

- Educate employees
- Flag emails from outside the organization
- Discuss social media use with team
- Establish multi-step verification for all requests for sensitive date or wire transfers
- Exercise data protection and data security policies
- Follow up phone call


[redacted]
13 July 2016 at 9:38 AM
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

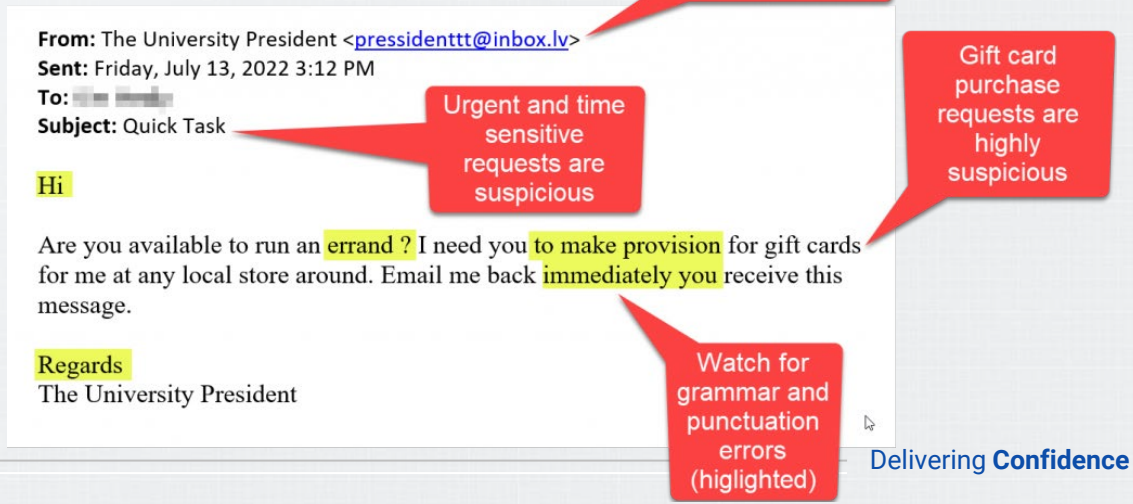
Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile



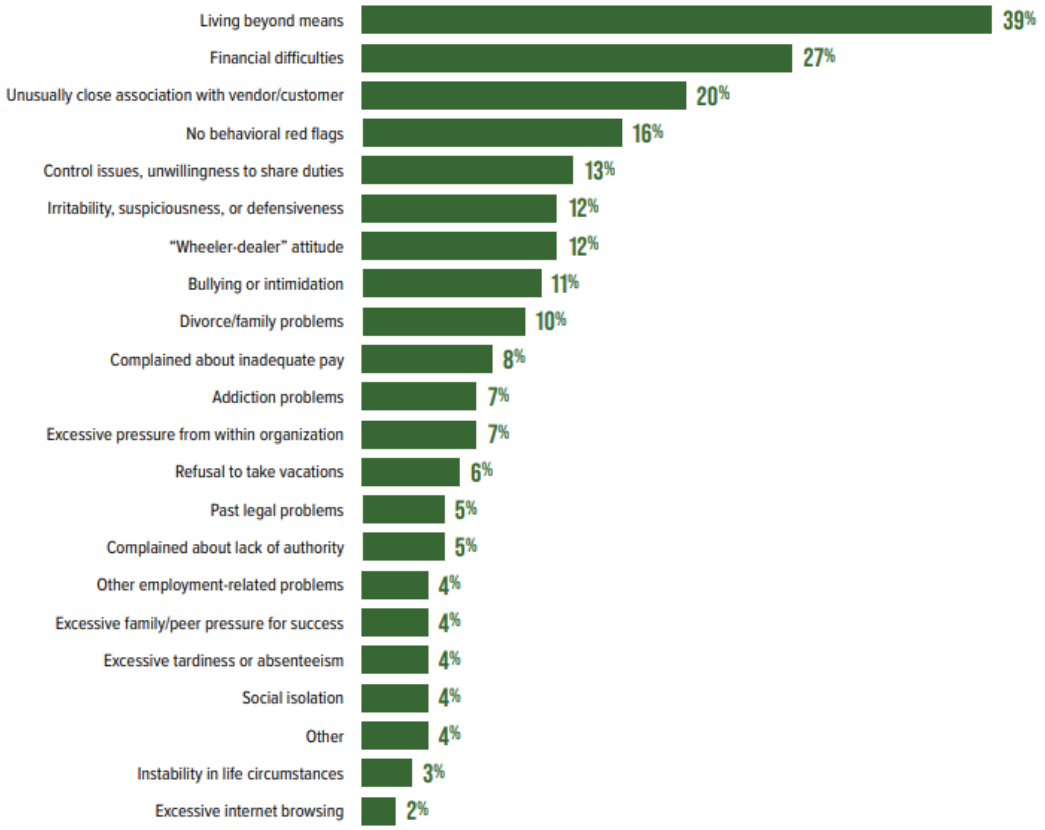
Know Your Scams

- Safeguarding user IDs and passwords
- Enabling two or multifactor authentication when possible
- Never clicking on communications from unknown sources
- Keeping current with hardware and software updates
- Be mindful of what you store on your devices and how you do it

BE SKEPTICAL!!

Look For Red Flags

FIG. 54 HOW OFTEN DO PERPETRATORS EXHIBIT BEHAVIORAL RED FLAGS?

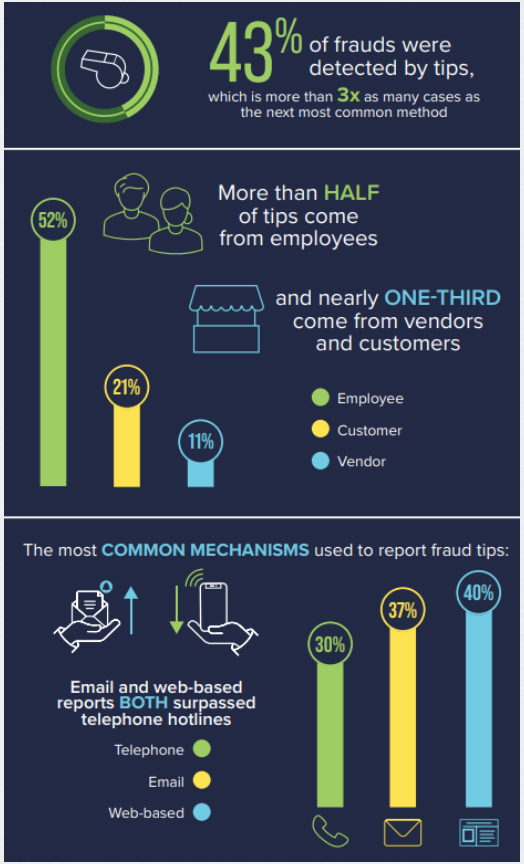


Fraud Prevention and Its Importance

- Fraud prevention is a process that's aimed to reduce loss in a firm 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.
- Preventing fraud from occurring in the first place is the most cost-effective way to limit fraud losses.



Fraud Prevention Checklist

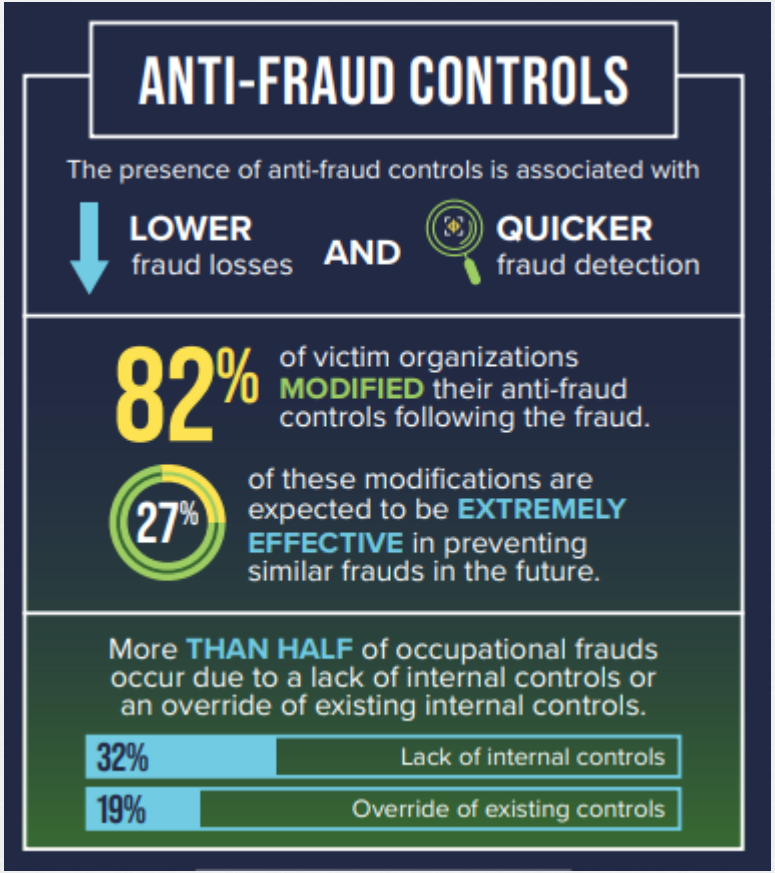
1. Is ongoing anti-fraud training provided to all employees of the organization?
2. Is an effective fraud reporting mechanism in place?
3. To increase employees' perception of detection, are the following proactive measures taken and publicized to employees?
4. Is the management climate/tone at the top one of honesty and integrity?
5. Are fraud risk assessments performed to proactively identify and mitigate the company's vulnerabilities to internal and external fraud?
6. Are strong anti-fraud controls in place and operating effectively?
7. Does the internal audit department, if one exists, have adequate resources and authority to operate effectively and without undue influence from senior management?
8. Does hiring practices include checks?
9. Are employee support programs in place to assist employees struggling with addition, mental/emotional health, family or financial problems?
10. Is an open-door policy in place that allows employees to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?
11. Are regular, anonymous surveys conducted to assess employee morale?

Establish Anti-Fraud Culture – Fraud Policy

The tone from the top is a key part of any fraud prevention and detection strategy.

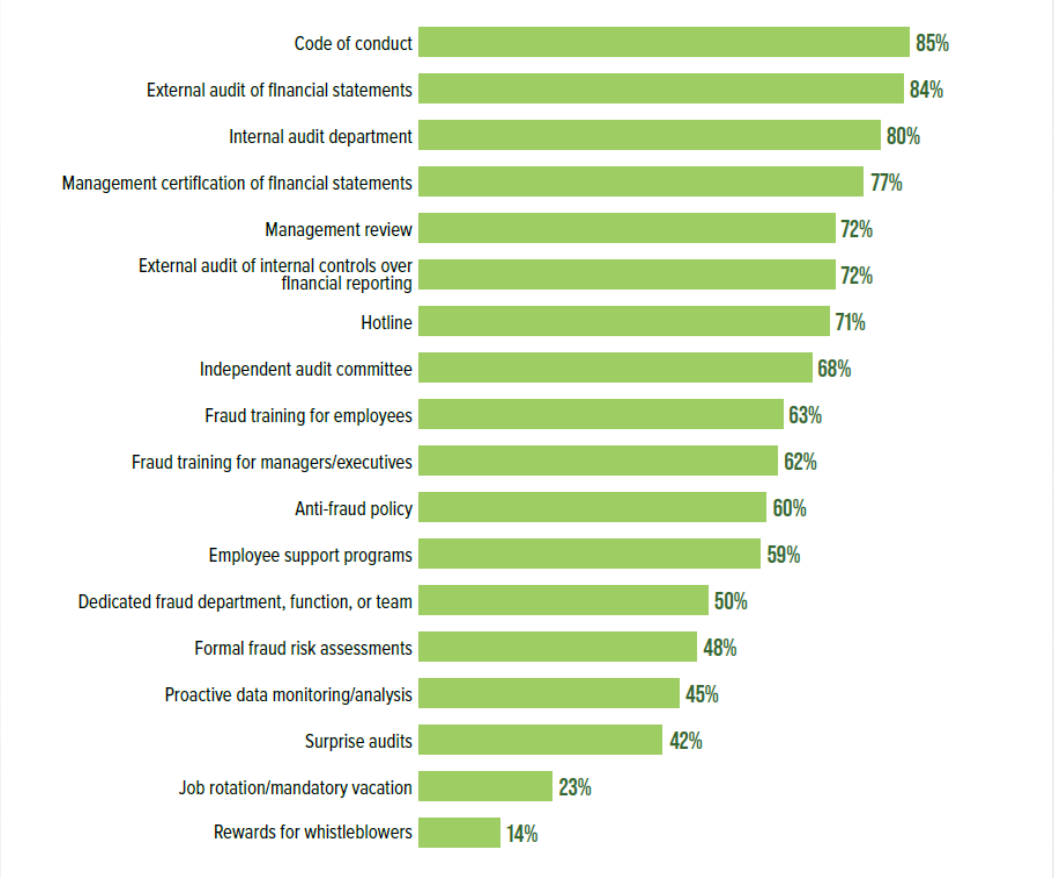
A fraud policy should include these key elements:

- An explicit definition of actions that are deemed to be fraudulent
- Allocation of responsibilities for the overall management of fraud
- A statement that all appropriate measures to deter fraud will be taken
- The formal procedures which employees should follow if a fraud is suspected
- Notification that all instances of suspected fraud will be investigated and reported to the appropriate authorities
- An unequivocal statement that all fraud offenders will be prosecuted and that the police will be assisted in any investigation that is required
- A statement that all efforts will be made to recover wrongfully obtained assets from fraudsters
- Encouragement to employees to report any suspicion of fraud
- The steps to be taken in the event a fraud is discovered and who is responsible for taking action



The Importance of Providing Fraud Awareness Training

Anti-Fraud Controls at Victim Organizations



Social Media

Failing to prioritize the security and privacy of a social media account can result in negative consequences spanning both the personal and professional worlds.

By asking seemingly random questions, malicious actors can use social engineering to obtain the information necessary to answer security questions required to reset a password (e.g., the name of a first pet, mother's maiden name).

For example, a malicious actor could leverage information gleaned from social media accounts about an upcoming class reunion. Posing as a classmate, the malicious actor could increase the likelihood of success in an email compromise through the use of a tailored phishing email campaign. This believable impersonation effort would allow the threat actor to gain the trust of the target account holder and leverage it for malicious purposes.

Practice Good Cyber Hygiene

Cyber hygiene is a set of best practices organizations perform regularly to maintain health and security of users, devices, networks and data.

- Passwords
- Multifactor authentication
- Secure your network firewall
- Anti-malware and antivirus programs
- Update operating systems and apps
- Get a reliable VPN
- Backup your files
- Delete suspicious emails or messages
- Completely remove all data from old devices
- Stay on top of your cyber security

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

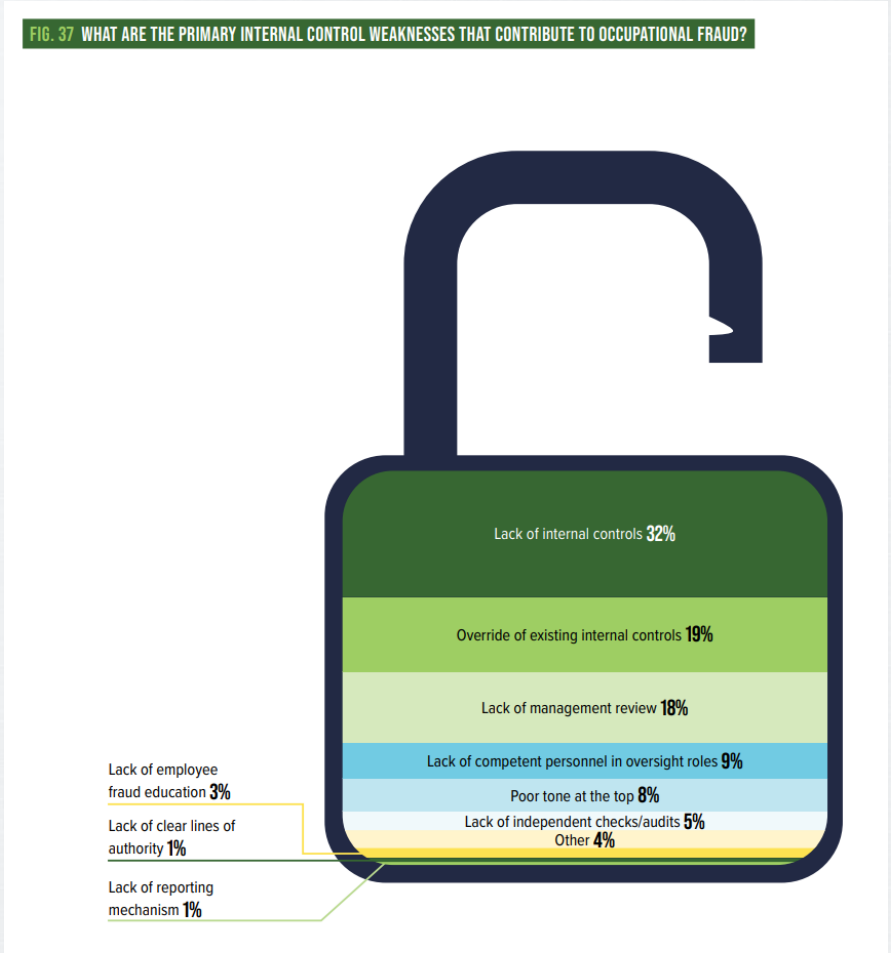
Separate Financial Duties

Many small to medium size business owners and employees have multiple duties and responsibilities

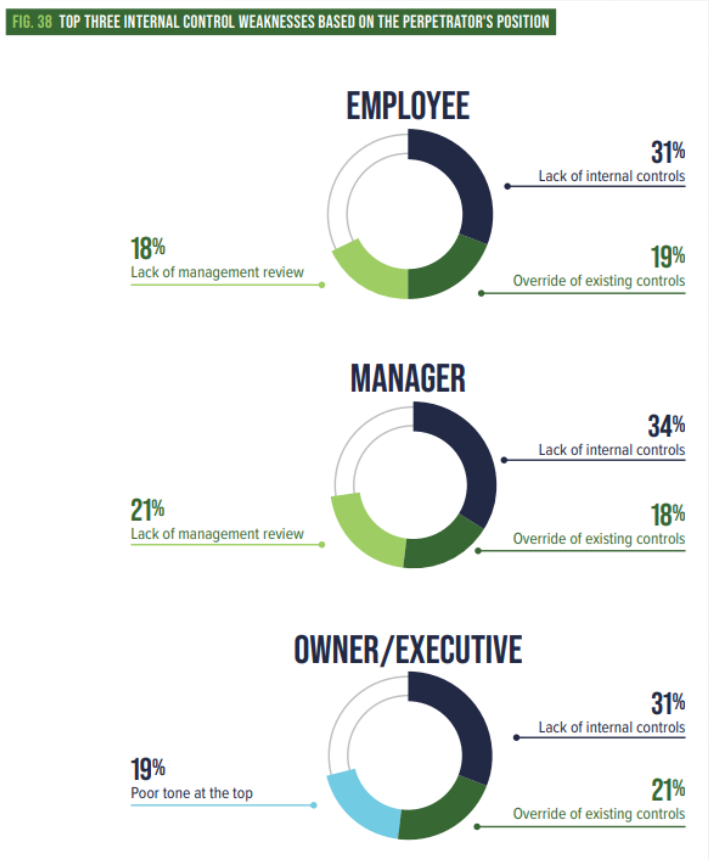
- Quote, negotiate, accept and reconcile payments with customers
- Enter, process and pay payroll
- Calculate and complete deposits
- Request and approve purchases

This introduces two risks:

- Risk of error
- Risk of theft



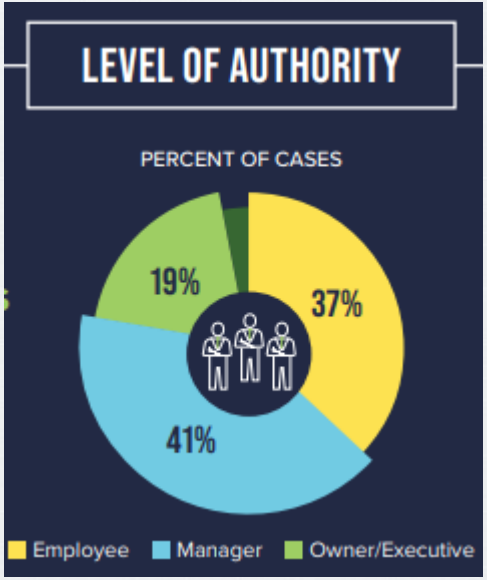
Separate Financial Duties



- 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

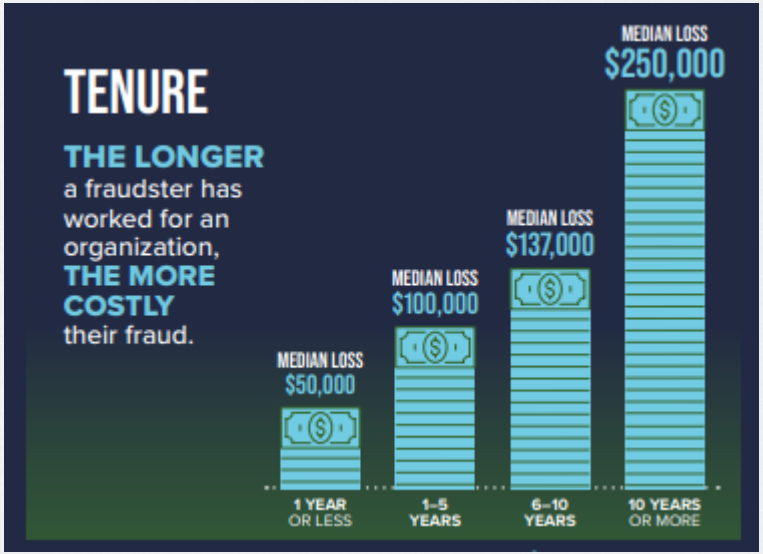
Restrict Access to Financial Systems and Data

- 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 entered payroll or given deliverable to 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

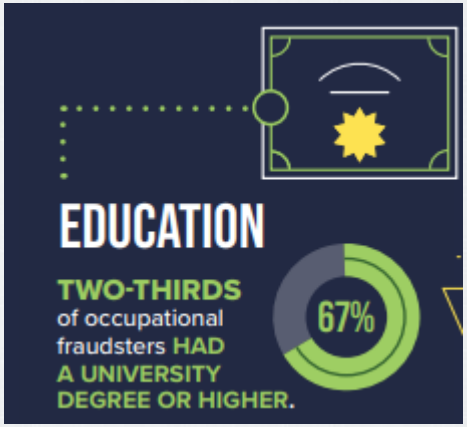


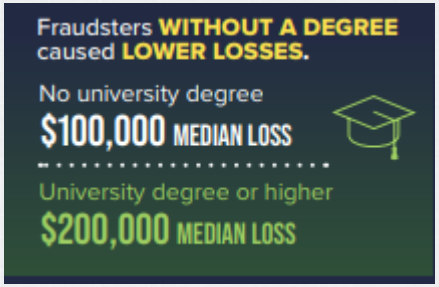
Randomize Reviews

- 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.



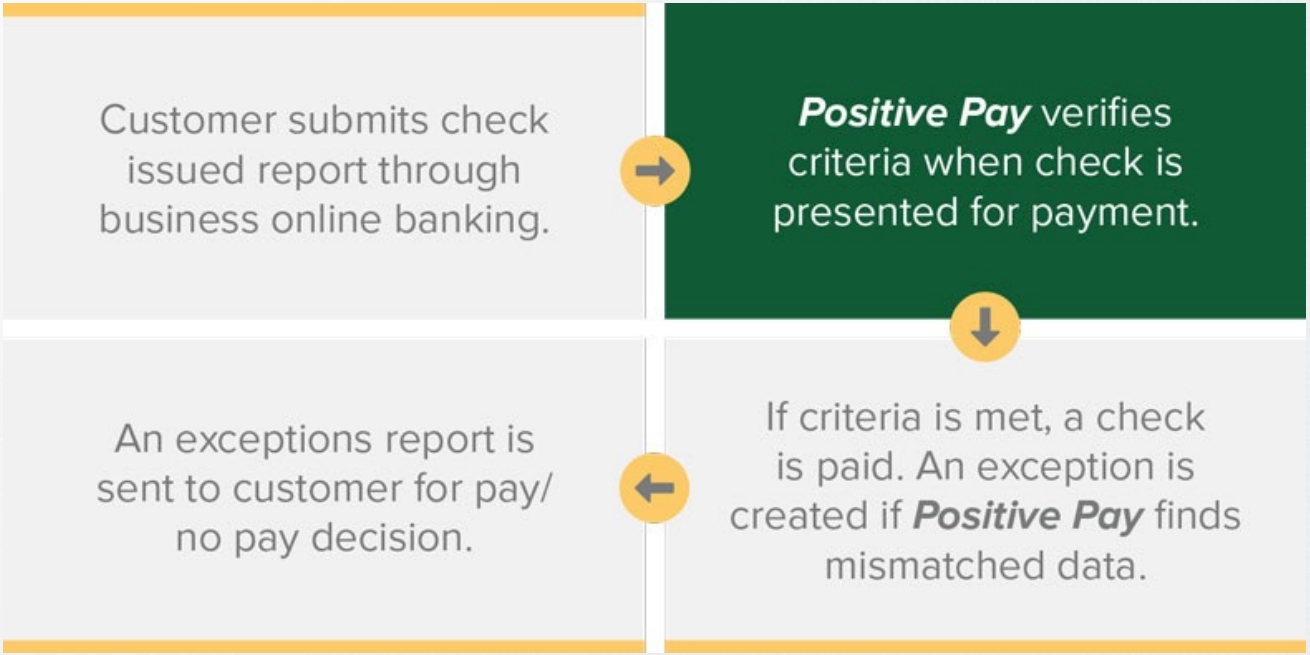


Additional Controls to Implement

- 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

Best Practices to Implement

Consider Implementing Positive Pay - Positive Pay is an automated Cash-management service used by financial institutions to deter check fraud.



Best Practices to Implement

- **Train staff regularly:** Online security training should be a regular occurrence that includes all staff across the organization, including volunteers with online access.
- **Protect passwords:** Instruct staff to change passwords often or put software in place that requires passwords to be changed and stress the importance of not recycling passwords across multiple websites and social media platforms.
- **Update software regularly:** At a minimum, systems should have strong spam email filtering, antivirus software and financial malware detection software. This software should be updated and patched regularly for the best defense

Best Practices to Implement

- **Regularly backup systems:** Maintain regular backups of critical data to protect against system failure and ransomware attacks. Disconnect external backup drives from your machine when not in use.
- **Restrict privileges:** Limit the number of people who have administrative privileges that allow them to make changes to systems. The more people who have access to this ability, the greater chance of a cybercriminal obtaining these sensitive credentials.
- **Use multi-factor authentication:** Require that users enable multifactor authentication when signing into their online accounts.

Best Practices to Implement

Consider Outsourcing IT Services - Firms don't always have a dedicated IT employee – by outsourcing IT functions, key personnel can focus on the mission and leave the cyber security and other imperative IT functions to the experts.

Best Practices to Implement

- **Verbally validate payment instructions:** It's always best to pick up the phone and communicate with the relevant parties to confirm requests.
- **Create a disaster recovery plan:** The actions and corresponding roles to take if systems are compromised should be clearly documented and understood.
- **Consider an insurance policy:** Insurance for cybersecurity typically includes first-party coverage of losses incurred through data destruction, hacking, data extortion, and data theft. Policies may also provide coverage for legal expenses and related costs.

Free Resources

- FBI
- Cybersecurity and Infrastructure Security Agency (CISA)
- ACFE
- AICPA

ACFE®
Association of Certified Fraud Examiners

U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE

AICPA®

Questions

Kaitlyn H. Axenfeld, CPA/CFF, CFE
Audit Partner

Email: kaxenfeld@dmcpas.com

Web: www.dmcpas.com

Address:

DM Financial Plaza
221 S. Warren St.
Syracuse, New York 13202-1628

Phone: (315) 472-9127, ext. 207

Copyright / Disclaimer

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.