DANNIBLE & MCKEE, LLP

Certified Public Accountants and Consultants

Delivering **Confidence**

Fraud: It's Still Here

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

November 6, 2024

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

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 Do People Commit Fraud?

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

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

Warning Signs

Most Common Types of Fraud Affecting Businesses

Asset Misappropriation

- Theft or misuse of company assets
- Examples: Embezzling cash, falsifying expense reports, stealing property

Financial Statement Fraud

- Manipulating financial records to misrepresent a company's financial health
- Examples: Overstating revenues, underreporting expenses

Corruption and Bribery

- Offering or accepting gifts, payments, or favors for preferential treatment
- Examples: Kickback schemes, vendor favoritism

Cyber Fraud

- Using technology to commit fraud, often targeting sensitive data
- Examples: Phishing attacks, data breaches, identity theft

Know Your Scams

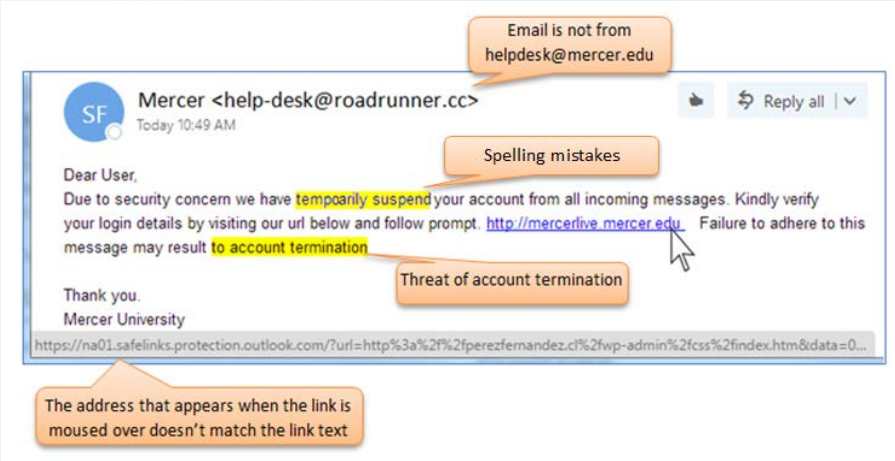
Each of these scams is carried out with the goal of tricking the victim into providing information or clicking on a link, which will install malware onto their device:

- 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:

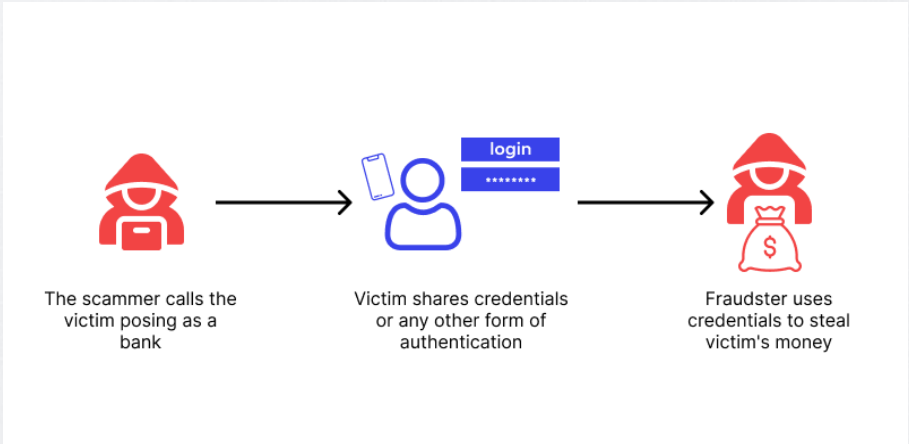
- Be aware
- Don't give into pressure
- Don't answer phone calls from unknown numbers
- Stay calm
- Be skeptical

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

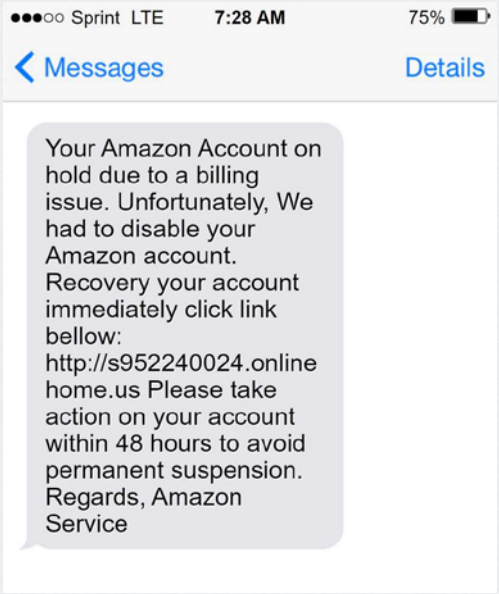
Smishing - scam carried out via text or social media

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

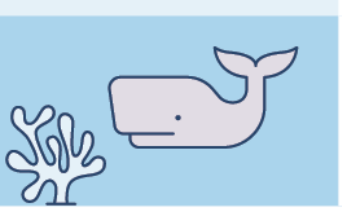
Phishing vs. spear phishing vs. whaling

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

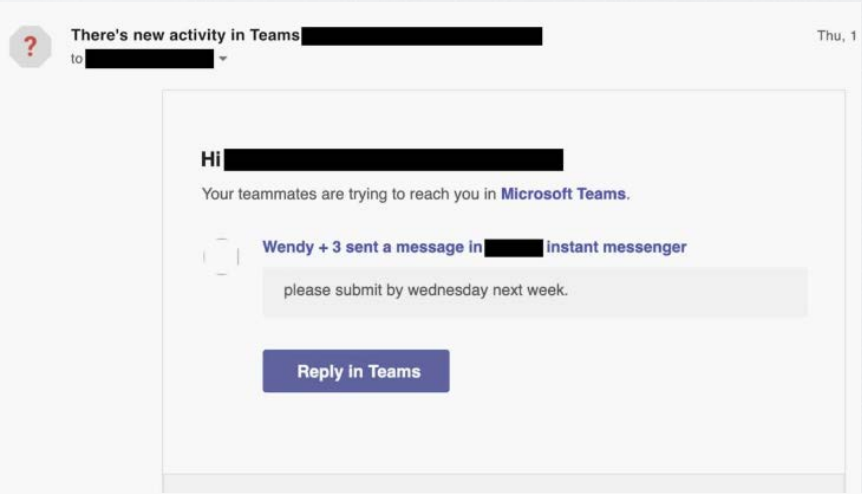
Spear Phishing - targeted phishing, in which the fraudster takes time to learn about the victim.

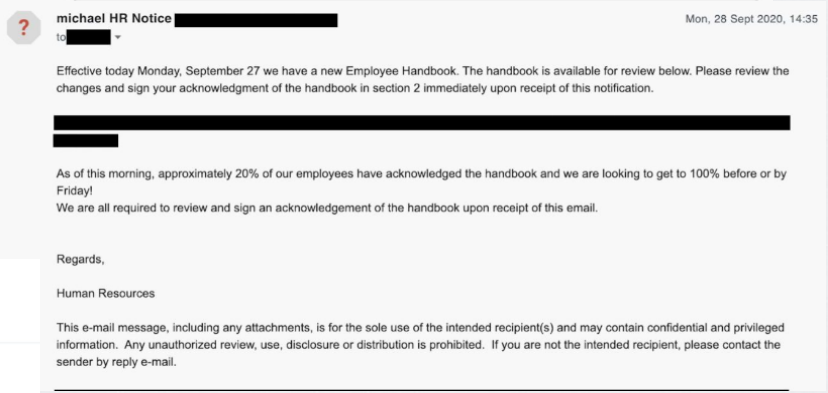
Personalized emails to particular individuals or groups of people with something in common.

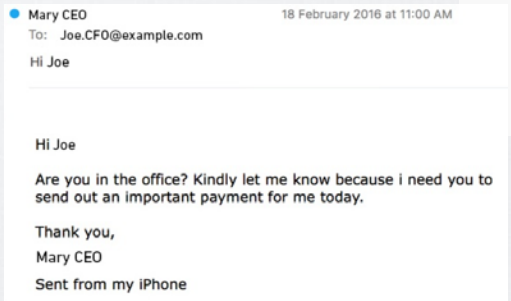
Sole purpose is to get inside the recipient's head and make them think the messages they're responding to are 100 percent legitimate—achieved due to personal touches designed to make them think what they're dealing with is the real deal.

Prevention:

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







Know Your Scams

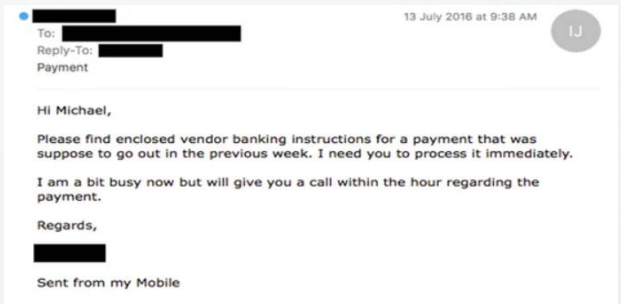
Whaling - targeting executives or presidents with the hope for a bigger return on the phishing investment.

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,

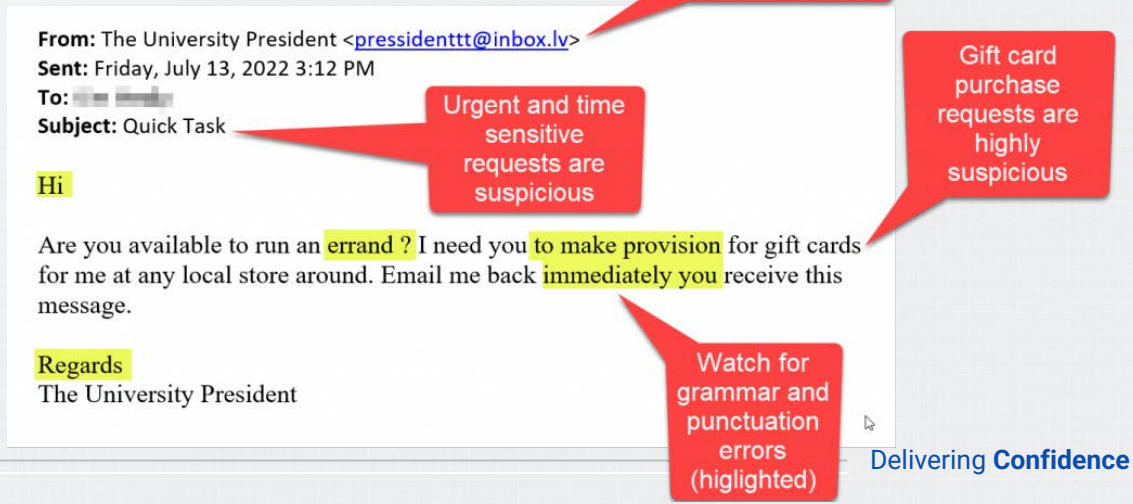
Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

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

Regards,

[redacted]

Sent from my Mobile



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.

Know Your Scams

- Safeguarding user IDs and passwords
- Enabling two or multifactor authentication when possible
- Never clicking on communications from unknown sources
- Running training simulations for phishing, vishing, smishing, spear fishing, whaling and business email compromise
- Keeping current with hardware and software updates
- Be mindful of what you store on your devices and how you do it

BE SKEPTICAL!!

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.

Recent Fraud Case Studies

Case 1 Overview – Wegmans

- Alicia Torres, a 48-year-old employee from Webster, NY, who worked for Wegmans
- Torres stole approximately $578,943.86 by manipulating the store's prescription system
- The fraud occurred over nearly a decade. It went undetected and the damages built up overtime.

How It Happened: Wegmans Case

- Alicia Torres manipulated Wegmans' prescription system to generate fake refunds. She used her access to system to look up recent customer transactions.
- She would then create false refund requests based on the previous customer transactions she observed, using actual customer’s names and recent prescription orders to make the request appear legitimate.
- Torres would then have a pharmacist sign off on the refund.
- After the pharmacist authorized it, Torres would swipe her bank debit card in Wegman's point of sale system to send the funds to her account.
- Between 2014 – 2023, Torres processed 350 credit card requests in customers' names with fictitious amounts.

How It Happened: Wegmans Case

- Torres exploited the fact that she could create a false invoice, and then could also be the one processing it, after tricking a pharmacist to sign off on it
- Wegmans lacked execution of adequate monitoring and auditing mechanisms for the refund process, allowing Torres to create and process 350 refunds through the pharmacy, basically without question
- The absence of other employees being a part of the refund process allowed Alicia to manage most of the refund processes herself

Red Flags: Wegmans Case

- **Unusual Refund Patterns:** A high frequency of refunds processed by a single employee over time should have raised suspicion
- **Personal Financial Instability:** She told the FBI she began stealing funds after her son was born to help pay for medical bills and living expenses and she filed bankruptcy in 2014
- **Ineffective Control Procedures:** The fraud's nearly 10-year duration suggests a lack of regular, thorough audits of refund transactions and employee activities
- **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

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 and Takeaways

- Torres was sentenced to one year in prison after pleading guilty to wire fraud
- She is required to pay restitution to Wegmans totaling $578,944
- Wegmans issued a statement regarding the incident, saying “the press release is the result of an FBI investigation into a former Wegmans employee, who plead guilty to charges stemming from this investigation. As a company, we do not comment on employee separations.”

Case 2 Overview – St. Amelia Church

- Lisa Noble, the business manager of St. Amelia Church in Tonawanda, NY
- Noble is under investigation for the alleged theft of $465,000 in church funds
- The missing funds were discovered during a routine audit by the Buffalo Diocese after the church noticed discrepancies in its bank statements
- As of early 2024, the investigation is still ongoing, with the amount of missing funds under scrutiny

How it Happened: St. Amelia Church Case

- Lisa Noble had full control over the church's financial accounts. She used her position to access and divert funds from the church’s bank accounts.
- She likely manipulated or falsified bank statements and internal financial records to conceal the missing funds. This included potentially altering transaction details to cover her tracks.
- The fraud continued for several months before discrepancies were noticed, indicating that Noble was able to conceal the fraud through manipulation and misreporting. The church did not conduct regular or thorough reviews of its financial statements, allowing her actions to go unnoticed.
- Noble’s control over both financial transactions and reporting created an opportunity for fraud without oversights from other parties.

Red Flags: St. Amelia Church Case

Discrepancies in Bank Records: Inconsistencies between bank statements and internal financial reports should have raised concern

Delayed Audits: The audit only occurred after discrepancies were discovered (reactive not proactive), suggesting a lack of regular financial reviews or ineffective internal controls

Access to Financial Records: Concentration of financial authority in the hands of one individual without oversight created a vulnerability to fraud

How the Fraud Could Have Been Prevented

- Regular reconciliation of bank statements with internal records could have detected the fraud earlier
- Separating the roles of fund management and financial oversight would have reduced the risk of fraud
- Regular Audits:
  - Conducting monthly internal audits over certain aspects of Noble's responsibilities to make sure everything was properly performed (for review of both fraud and accuracy)
  - Conducting independent, external audits or other engagements with an independent CPA Firm on an annual basis would provide an unbiased review of the church’s finances and highlight irregularities sooner.

Case 3 Overview – CNY Premier Soccer Club

- Paul R. Palucci, 36, president of the CNY Premier Soccer Club
- Palucci embezzled over $55,000 from the soccer club by making fraudulent charges on the organization's accounts
- He falsified business records to cover up the personal expenses charged to the club's accounts
- Palucci was charged with second-degree grand larceny and first-degree falsifying business records

How It Happened: CNY Premier Soccer Club Case

- Paul R. Palucci used the soccer club's accounts to make fraudulent charges. He likely used club funds for personal expenses or unauthorized purchases.
- To cover up these transactions, Palucci falsified business records, making personal expenses appear as legitimate club-related costs.
- As president of the club, Palucci had significant control over financial decisions without sufficient oversight, which facilitated his fraudulent activities.
- The absence of a dual approval process for expenses allowed him to make unauthorized transactions without examination.
- Weak Financial Monitoring: The club lacked rigorous financial monitoring, which failed to detect and prevent the misuse of funds.

Red Flags: CNY Premier Soccer Club Case

Unexplained Expenses: Irregularities in the club's expenses, such as charges that couldn't be tied to club activities, were not questioned early on

No Dual Approval Process: Palucci had sole control over financial decisions without requiring approval from others

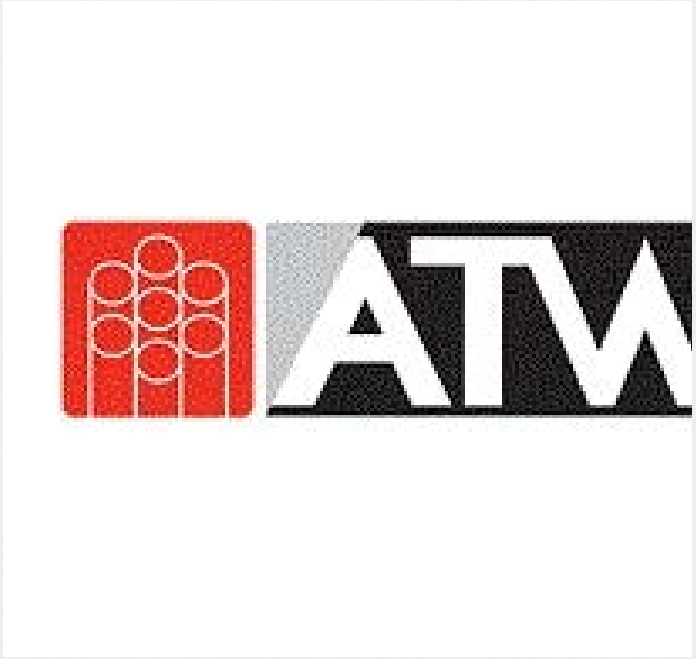
Missing Financial Records: Inconsistent or missing documentation of purchases and expenses, which should have raised concerns about financial mismanagement

How the Fraud Could Have Been Prevented

- Requiring dual approval for expenses would have created a system of checks and balances, reducing the chance of unauthorized spending
- Conducting regular reviews of financial records would have flagged unusual transactions earlier
- Segregation of Duties: Separating financial authority, so no one person controlled the accounts, would have added another layer of protection

Case 4 Overview – Rhode Island Metals Fabrication Company

- Juan Hicks, 47, the IT Director of a Rhode Island-based metals fabrication company.
- Hicks embezzled over $1 million from his employer over a 10-year period by using his purchasing authority to make unauthorized purchases for personal use.



How It Happened: Rhode Island Metals Fabrication

Juan Hicks, as IT Director, used his purchasing authority to make personal purchases, which he charged to the company's accounts.

- Created false invoices and expense reports for purchases that were never made
- Altered credit card statements to make purchases appear to be business expenses, when they were for personal purchases
- Issued company phones to himself and 6 family members and then enrolled the phones on the Company's wireless phone service plan
- Submitted invoices and used company credit cards to purchase airline and entertainment tickets for himself, family members and friends
- Used company credit cards to make purchases at retail and auto stores for personal expenses

Over a period of about 10 years, Hicks stole over $1 million for personal use through the above tactics.

How It Happened: Rhode Island Metals Fabrication

- Hicks' conduct came to light in March 2022 when his employer hired forensic analysts to find the source of a cyberattack and assess the vulnerabilities in the Company's computer system.
- These independent analysts quickly found irregularities that started to point to Hicks and their information and analysis was provided to the Police, Homeland Security and US Attorney's Office who further investigated and revealed over $1,000,000 had been stolen

Red Flags: Rhode Island Metals Fabrication Case

Unexplained Purchases: Hicks made unauthorized purchases that weren't questioned, indicating a lack of scrutiny in the approval and review process surrounding the company's expense reimbursement process and use of company issued credit cards.

Absence of Regular Reviews: The lack of regular reviews of purchases and financial records allowed the fraud to continue unchecked. Who was reviewing the company credit cards? Who reviewed and approved expense report reimbursement requests?

- What was the lifestyle Hicks lived compared to his compensation at the company?

How the Fraud Could Have Been Prevented

- Implementing more stringent internal controls over purchasing and financial transactions would have helped prevent the fraud.
- Regular audits and reviews of purchase orders, company credit card statements and other financial records could have detected the fraud earlier.
- Putting a limit on expense reimbursements or implementing a system of approval for all purchases after an employee exceeds a certain annual dollar amount

Conclusion

- Hicks was sentenced to three years in prison after pleading guilty to wire fraud.
- Hicks will also serve three years of federal supervised release after serving his sentence.
- He is required to pay restitution to ATW Companies totaling $1,042,000.

Common Red Flags and Warning Signs

Common Red Flags and Warning Signs

Common indicators from the cases:

- Sudden lifestyle changes in employees
- Living beyond means
- Divorce/Family issues
- Financial pressure
- Discrepancies in financial records
- Unusual activity on company credit cards

Tips to Safeguard Your Business

Why is Fraud Prevention Important?

- Every year tons of money is lost to fraud and increasing 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.

Fraud Prevention Strategies

- Implementing strong internal controls.
- Regular audits and reviews of internal controls.
- Segregation of duties.
- Employee training and education.
- Importance of fraud awareness.
- Creating a culture of transparency.
- Encouraging ethical behavior and whistleblowing

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 including:
  - procedures staff should follow
  - assigning responsibility for an instant response to the occurrence recovering funds
  - dealing with the media
  - preserving evidence and reporting to the police

A fraud policy raises awareness amongst staff that response plans have been devised, to deal with and minimize the damage caused by any fraudulent attack. By explicitly defining actions that constitute fraud you ensure that all employees and third parties are aware of what is and is not acceptable.

Prioritize Fraud Program Documentation

- Often, there are gaps in documentation related to fraud definitions and examples, roles and responsibilities across the organization and program governance.

- These gaps can lead to program pitfalls. For example, a lack of sufficient detail related to roles and responsibilities can lead to several problems:
  - Redundancy (same tasks being completed by multiple teams in different ways, causing downstream confusion)
  - Lack of cohesive understanding of the program and who does what
  - Key fraud controls and activities lacking a clear owners, leading to those activities not being performed or being performed in an ad hoc manner
  - Confusion across the organization about how to raise potential fraud concerns to the right people

- The Fraud Program should ultimately be the road map outlining strategic priorities, ongoing initiatives, and future enhancements; defining a clear approach to measure the success of the strategy and its underlying initiatives.

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.

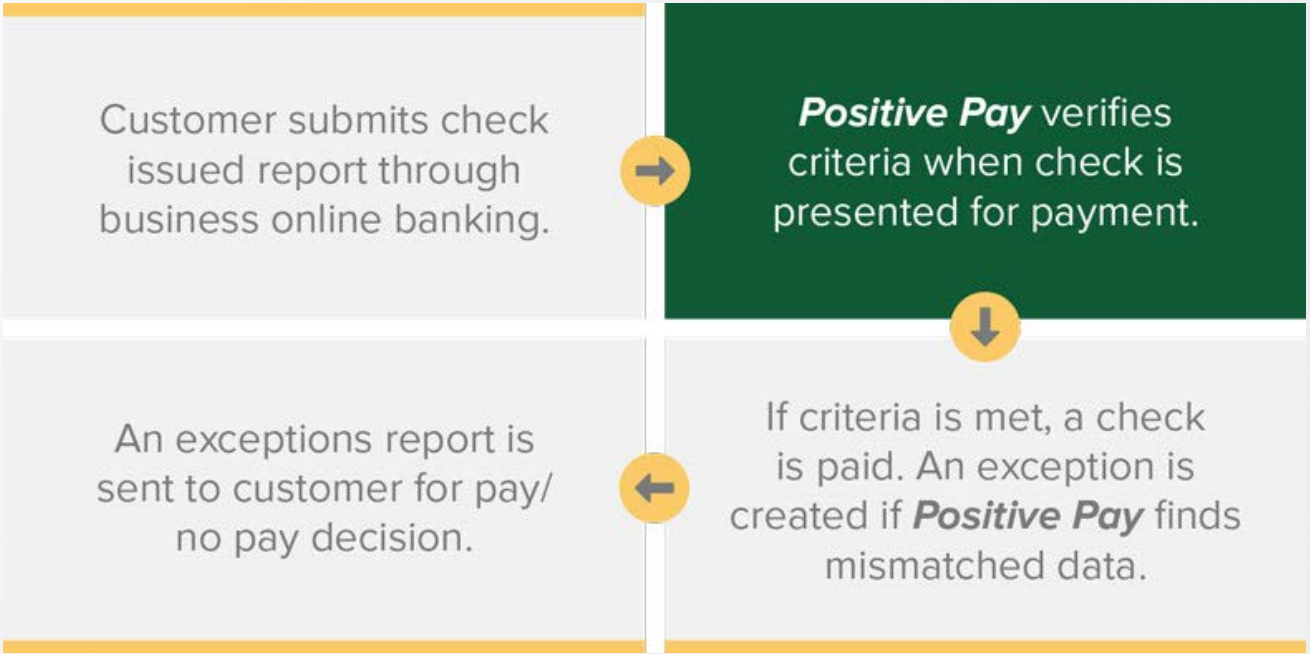
- Passwords
- Multifactor authentication
- Secure your network firewall
- Anti-malware and antivirus programs
- Update operating systems and apps
- Get a reliable VPN
- Backup your server/files
- Delete suspicious emails or messages
- Completely remove all data from old devices
- Stay on top of your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

Data Breaches Still Happen

National Public Data experienced a massive data breach affecting 2.9 billion records, including Social Security numbers and contact information, after a December 2023 cyberattack by the USDoD group. The stolen data, posted on the dark web in April 2024 with a $3.5 million price, led to a class-action lawsuit due to unencrypted data exposure.

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

RISK TERMINOLOGY

THREAT: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, assets, individuals, other organizations, or society

VULNERABILITIES: A characteristic or specific weakness that renders an organization or asset open to exploitation by a given threat

LIKELIHOOD: Refers to the probability that a risk scenario could occur

RISK: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences

- **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

- **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.

Best Practices to Implement

Consider Outsourcing IT Services - Companies 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.

Free Resources

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

ACFE®
Association of Certified Fraud Examiners

CISA
CYBER+INFRASTRUCTURE

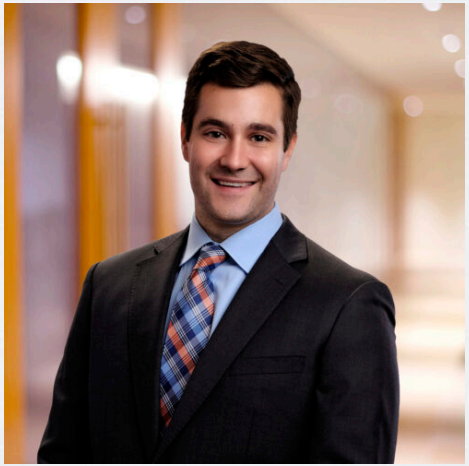
AICPA®

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

Kaitlyn H. Axenfeld, CPA/CFF, CFE
Audit Partner
kaxenfeld@dmcpas.com



Robert C. Reeves, CPA, CFE
Audit Partner
rreeves@dmcpas.com

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.