Embezzlement & Fraud

How You Can Protect Yourself

Pam Newman, CMA,CFM, MBA

Pam Newman

- BS and MBA from University of Nebraska
- CMA – Certified Management Accountant
- CFM – Certified Financial Manager
- President of RPPC, Inc (Realizing Profitable Potential through Change)
- Author of ***Out of the Red*** and ***Boost Your Bottom Line***
- Contributing writer for various publications and sites, including www.Entrepreneur.com
- Radio Spokesperson for QuickBooks® Small Business Campaign

Definitions

- Embezzle:
  - to appropriate fraudulently to one's own use, as money or property entrusted to one's care.
- Fraud:
  - deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.

It CAN happen to you

- Most businesses don't think it will happen to them because they
  - Hire friends/family
  - Don't have "that much" money
  - Don't believe they have "inventory" that people can remove from the premises.
- What's your belief?
- Raise your hand if you or someone you know has a business that has been impacted by embezzlement.

5 Most Common Types of Fraud

- Skimming – A sale is made but not recorded and payment is taken personally.
- Payroll Fraud – Fake employees or false documenting of hours.
- Inventory Fraud – Anything can disappear.
  - pens/paper/merchandise/machinery parts/etc.
- Fraudulent Disbursements – Payments made against phony bills.
- Checkbook Fraud – Using company funds for personal use.

(http://www.aw-wrdsmith.com/FAQ/14_Steps_for_Preventing_Fraud.html)

Environment Conducive to Fraud

- Overbearing management with no checks and balances.
- Climate of fear.
- High staff turnover rates in key controlling functions.
- Long-service staff in stores/purchasing departments.
- Major understaffing in key control areas.
- Frequent changes of outside professionals such as attorneys and accountants.
- Failure of proper analysis of data.
- Lack of common-sense controls such as changing passwords frequently, requiring two signatures on checks, or restricting access to sensitive areas.

Environment Conducive to Fraud

- Inadequate segregation of duties.
- Past rumors of fraud not dealt with effectively, or at all.
- Inadequate internal reporting or management accounting.
- Poor staff morale / lack of career progression / weak management.
- Excessive pressure to meet budgets, targets, or forecast earnings.
- Personnel not required to take time off and cross train others to do their jobs while gone.
- An employee's personal situation changes (spouse's loss of job, sick family member, etc).

Resource: http://www.tradeangles.fsbusiness.co.uk/articles/fraud_detection.htm

Prevention

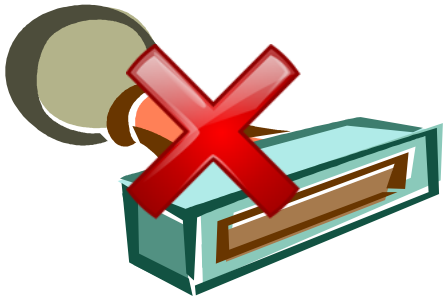
- Key is protecting yourself, and your employees, by having protective measures in place.
- What assets do you have that could easily disappear?
  - Cash
  - Inventory
  - Information
- Secure your premises – both physical and informational.
  - Security Cameras
  - Restricted access to cash, inventory, and information
  - Checks and balances in the day-to-day activities of your organization

Cash

- Don't leave cash laying around.
- Even the most honest person can be tempted by an appearance that you have so much money that you don't need to keep tabs on it.
- There should be two people handling cash activities for their protection and yours.
- Don't have more than $50 petty cash in office.
  - Require receipts for all expenditures.
- Implement surprise reviews to test for lapses in security.
  - Internal Management
  - Outside Accountant

Signature Stamps

- Absolutely NOT!
- These are a disaster waiting to happen when someone can get hold of your signature stamp.
  - If you feel the need to have one, keep them locked up.

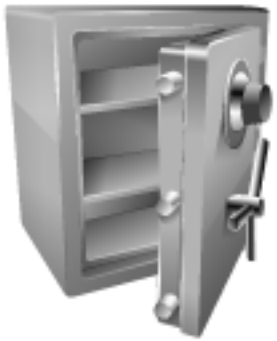


Bank Account

- Limit the number of people who have access to your bank accounts.
- Keep checks in locked safe.
- Too much information can be a temptation.
- Reconcile bank accounts every month.
  - Person reconciling should be different then person signing checks and entering into computerized bookkeeping system.
  - Surprise reconciliations by your accountant.
  - Have the bank account statements sent to a different location so you have the chance to review them before anyone at the office.
- For large amounts, checks should require dual signatures.

Deposit Regularly

- Don't leave cash or checks laying around the office.
  - They need to be in a locked safe until taken to the bank.
- Deposits should be made daily, if there are large amounts of checks or cash.
- Use locked or sealed bags so that when they are being delivered to the bank no one has access to them.



Payroll

- Most common types of payroll fraud are fictitious employees and/or falsifying hours.
- Have an authorized person sign off on all payroll timesheets that are turned in.

Cross Train Employees

- A good business model should incorporate cross training of employees, so that every position has a backup.
  - This allows the company to have the ability to do surprise substitutions of various positions.
  - Provides a backup for availability during vacations, sick time, and in the event that a position becomes vacant.
  - Mandate vacations so that other people do the work – it can minimize opportunity for fraudulent activity.
    - If you have employees that never take vacation – you may be creating the environment for fraud, as they never have anyone covering their activities.
    - Make it mandatory for employees to take a minimum of 1 week off at a time so someone else HAS to do their work.

Bonding

- Any employee that will be handling cash should be bonded.
- People considered at risk:
  - **Ex-offenders**, including anyone with a record of arrest, conviction, or imprisonment, and anyone who has ever been on probation or parole.
  - **Ex-addicts** (persons with a history of alcohol or drug abuse).
  - Persons having a **poor credit record** or who have declared bankruptcy.
  - **Economically disadvantaged persons who lack a work history**.
  - Individuals who were **dishonorably discharged from the military**.
  - Others who experience a barrier to gaining employment, due to their personal background.
- What is the benefit of a bond:
  - The bond insurance reimburses the employer for any loss due to employee theft of money or property.
  - There is no deductible amount (i.e., 100% bond insurance coverage).

Background Checks

- Different types of information – you need to determine what is important for you to know.
  - Criminal Checks
  - Credit Reports
  - Driving Record
  - Educational Background
- Check References of EVERY employee.

Separation of Functions

- There should be a checks and balances system within your organization.
  - Completing work/invoicing/receiving payment
  - Entering bills/paying bills/signing checks
  - Deposits/Checks/Reconciling
  - Purchase Orders/Receiving of Inventory
- The goal is to minimize opportunity for fraud.
- Every purchase should have a purchase order signed by an authorized person.
  - Limit who has authorization to make purchases and set dollar limits.

Establish 3rd Party Hotline Service

- #1 way to catch occupational fraud are your employees.
  - Most employees are reluctant to report suspicious activity. Utilize a third-party hotline which offers a level of anonymity that an in-house hotline might not provide.
  - Therefore, employees will be more likely to blow the whistle on fraudulent activity if they feel their identity is protected.
  - An outside company is staffed 24 hours a day and provides information to the business immediately.

What if it's happened?

- Contact your local police, accountant, and attorney to understand your options.
  - Your IT person may also need to be involved, depending on what type of fraudulent activity has taken place.
  - There are accountants that are specifically trained in fraud investigation. They are referred to as forensic accountants and are most likely found at your bigger accounting firms, due to the specialization of services they provide.
- You must take precautionary steps to protect any evidence.
- Immediately remove the person from the situation – specific advice should come from your personal contacts (attorney, police, & accountant) as they can be specific to your situation.

Overcoming

- The key is keeping cohesiveness within the organization when something unfortunate like this has happened.
  - You want to have communication so that people know the truth – you can pick how much detail you provide (usually minimal detail is the appropriate level to share).
    - If you don't share information then the rumors will run out of control. Control it.
- It is also important for you to have outside professionals assess exactly what your losses are and make specific recommendations on how to recover from this type of situation.
- If evidence is found to warrant taking legal action, expect that it will be a time consuming and expensive process.

Next Steps

- Listen to your professionals and implement recommended protection measures going forward.
  - Unfortunately too many wait until something has happened before they take it seriously.
- Understand it can happen more then once, so don't let your guard down.
  - It's never to late to implement controls for future protection, even though you cannot control past events.
  - It is imperative that you find a good balance, as you do not want to become paranoid to the point where you lose control, attempting to prevent something from happening.

Proactive vs. Reactive

- The best option is to be proactive in how you run your business, to prevent things like fraud and embezzlement from happening.
- If you are forced into reactive mode, because you have been the victim, you will find that you are caught trying to rebound.

Questions?

Anyone want to share their personal tips/experiences?

Contact Information:

- Pam Newman, CMA, CFM, MBA
- www.rppc.net
- 816.304.4398