THEFT, FRAUD AND CHEATING

FINANCIAL REPORTING FRAUD, EMBEZZLEMENT AND OTHER CYBER SCHEMES; HOW IT IS IDENTIFIED AND MEASURES TO PREVENT IT.

WELCOME

WILKE & ASSOCIATES

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

Wilke & Associates, CPAs & Business Advisors
1721 Cochran Road
Suite 200
Pittsburgh, PA 15220
(412) 278-2200

Carrie Reighard, CPA, MSA
creighard@wilkecpa.com

THREE TYPES OF FRAUD:

Misappropriation of assets

Employee/Insider theft, defalcation or embezzlement. This involves company assets and can be monetary or physical in nature.

Fraudulent financial reporting

Earnings management fraud. Intentional manipulation of accounting policies or estimates to improve financial statements.

Consumer fraud

False transactions or confidence schemes.

Misappropriation of Assets: Common Schemes

1. Authorized Check Maker – Ledger Editing
2. Forged Maker – Forged signatures, Signature stamp
3. Altered Check – Check Washing, Reproductions
4. Fraudulent Billing, Fraudulent Vendors
5. Inventory “shrinkage”
6. Payroll Fraud
7. Skimming
8. Expense Reimbursement Fraud

Misappropriation of Assets: Real World Examples

1. Matthews International - $13mm, 2017
2. Baierl Acura - $10mm, 2012
3. Quest Diagnostics - $1.2mm, 2008
4. Block Communications - $1mm, 1995
5. USPS - $40,000, 2008
6. Calgary Transit - $375,000, 2008
7. IKEA - $400,000, 2008
8. Quail Ridge Books & Music - $348,975, 2001

Consumer/Individual Fraud: Common Schemes

1. Confidence Schemes
2. Nigerian Prince
3. Phishing
4. Identify Theft
5. Credit Card Theft
6. Synthetic Identities
7. Telemarketing, Imposter Scams
8. Insurance Fraud
9. Mortgage Fraud

Consumer Fraud:
Real World Examples – 2017 (FTC)

1. Imposter Scams - $328mm
2. Debt Collection Scams – 2.7mm victims
3. Identity Theft – 1.1mm victims
4. Credit Card Theft, Wire Transfer – $74mm lost

Top States for Fraud (overall) – Florida, Georgia and Nevada

Top Identity Theft States – Florida, Michigan and California

Fraudulent Financial Reporting: Common Schemes

1. Earnings Smoothing
2. Improper Revenue Recognition, Fictitious Sales
3. Falsified Inventory
4. Channel Stuffing or Trade Loading
5. Misstating Liabilities
6. Fraudulent Post-Closing Entries
7. Check Kiting
8. Improper Valuation of Assets

Fraudulent Financial Reporting: Real World Examples

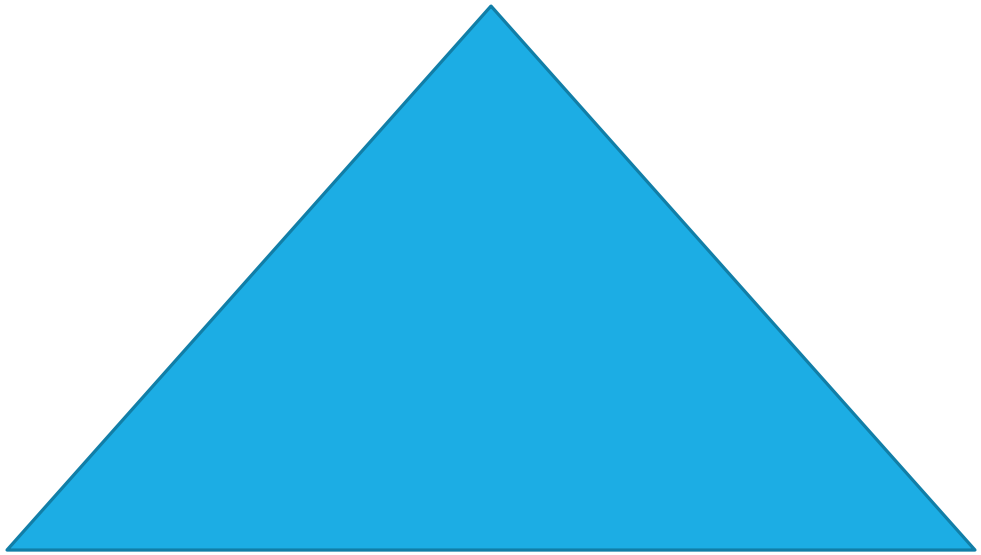
1. Enron, 2001
2. WorldCom, 2002
3. Sunbeam, 2002
4. Monsanto, 2011
5. Nortel, 2003

Identifying Fraud: Red Flags

- Financial Statement Anomalies, whole numbers
- Employee Actions
- External Communications
- Missing Documents
- Complaints
- Excess Transactions or Duplicates
- Inventory Shrinkage
- Abnormal Volume

Fraud Triangle

Incentives/Pressure



Opportunities

Attitudes/Rationalization

Fraud Triangle

Incentives/Pressures: Common incentive is declining revenues. Individuals will commit fraud in order to meet debt covenants, achieve bonus targets or inflate stock prices.

Opportunities: Accessible cash or valuable inventory especially if small or easily removed. Limited controls in the accounting environment.

Attitudes/Rationalizations: Attitudes, behavior expressed by top management – company culture. Motivations – external and internal.

Typical Profiles

- **Person of Good Standing**
- **Employed average of 5 years**
- **First time offenders**

Testing for Fraud

Financial Statement Analyses identify trends, changes and significant accounts.

Types of Analyses include:

- Horizontal Analysis
- Vertical Analysis
- Ratio Analysis

Horizontal Analysis—Income Statement

	20X3	20X2	Change	20X1	Change
Total revenues	$106,430	$53,557	98.7%	$22,603	136.9%
Total cost of goods sold	$19,781	$11,116	78.0%	$5,257	111.5%
Gross margin	$86,649	$42,441	104.2%	$17,346	144.7%
Operating expenses					
Sales and marketing	$53,408	$30,468	75.3%	$13,054	133.4%
Research and development	$12,106	$5,049	139.8%	$2,840	77.8%
General and administrative	$11,809	$6,552	80.2%	$3,742	75.1%
Total operating expenses	$77,323	$42,069	83.8%	$19,636	114.2%
Income (loss) from operations	$9,326	$372	2407.0%	($2,290)	(116.2)%
Provision for income taxes	($3,442)	—		—	
Net income (loss)	$6,178	$121	5005.8%	($2,375)	(105.1)%

Vertical Analysis—Income Statement

	20X3	20X2	20X1
Revenues	100.00%	100.00%	100.00%
Total cost of goods sold	18.59%	20.76%	23.26%
Gross margin	**81.41%**	**79.24%**	**76.74%**
Operating expenses			
Sales and marketing	50.18%	56.89%	57.75%
Research and development	11.37%	9.43%	12.56%
General and administrative	11.10%	12.23%	16.56%
Total operating expenses	**72.65%**	**78.55%**	**86.87%**
Income (loss) from operations	8.76%	0.69%	(10.13)%
Provision for income taxes	(3.23)%	—	—
Net income (loss)	5.80%	0.23%	(10.51)%

Ratio Analysis

- Means of measuring the relationship between two different financial statement amounts:
  - Accounts receivable turnover
  - Sales to total assets
  - Related-party sales to total assets
  - Working capital to total assets
  - Leverage ratios
  - Ratios involving nonfinancial data

HOW TO PREVENT CONSUMER FRAUD

- Spot Imposters, don’t believe Caller ID
- Do online searches, talk to people
- Strengthen passwords including your phone
- Don’t pay up front for a promise
- Consider how you pay
- Make liberal use of a shredder
- Hang up on robocalls
- Show proper skepticism
- Don’t deposit a check and wire money back
- Check credit reports frequently, monitor financial statements

HOW TO PREVENT FRAUD IN THE WORKPLACE

- Implement proper system of internal controls
- Properly segregate accounting duties among staff
- Perform background checks
- Make employees aware of new financial controls
- Rotate employees to various responsibilities
- Insist employees take PTO
- Scrutinize all business bank accounts
- Focus on improving a transparent and open-door corporate culture
- Train employees on fraud mitigation steps
- Know your business partners
- Get expert help

CREDIT CARD BREECHES

The only companies that are exposed to this are those that carry credit card account numbers and other personal identifying factors in their database.

Meaning within their own processes.

The companies we speak to contract out to third parties to process credit cards and don’t maintain them in a database that would be subject to a breech.

Most CIOs will be responsible for protecting Intellectual Property

IP Breeches

Previous Employees

Foreign Employees

IP Protection

1. Identify and Define what is your Intellectual Property
2. Where is your IP stored – Office machines, Cloud, Employee devices, 3rd Party
3. Secure you IP with policies and procedures – physically and electronically
4. Cost Risk Analysis to IP
5. Employ tools to protect your IP – Encryption
6. Play Devil's Advocate – How would you steal from your company
7. Everyone Around the world wants your client and employee information
8. Educate Employees
    1. Emailing-wrong addresses, forwarding messages and attachments
    2. File Sharing – Dropbox
    3. Messaging - SMS

Cybersecurity 5 Step Plan

Identify: Before an attack, identify what data or systems are vulnerable or could be stolen.

Protect: Safeguard data and systems with insurance and backups.

Detect: Be aware of any anomalies in your systems to detect a cyberattack as quickly as possible.

Respond: Take whatever action is necessary to stop the attack from continuing and contain the impact of the attack while managing communications with stakeholders like customers whose data may have been compromised.

Recover: Restore the capabilities and services that were disrupted for your business during the attack.

Cyber Liability Insurance

First Party Coverages:

- Loss or damage to electronic data
- Loss of income or extra expenses
- Cyber Extortion losses (ransomware)
- Notification costs
- Reputation Damage

Third Party Coverages:

- Network security liability
- Network privacy liability
- Electronic Media Liability

Thank You

Questions?