AUDIT TAX SYSTEMS ADVISORY

Financial Institutions Roundtable

A complimentary webinar series for financial institutions.

Fraud and Prevention Measures

April 30, 2014

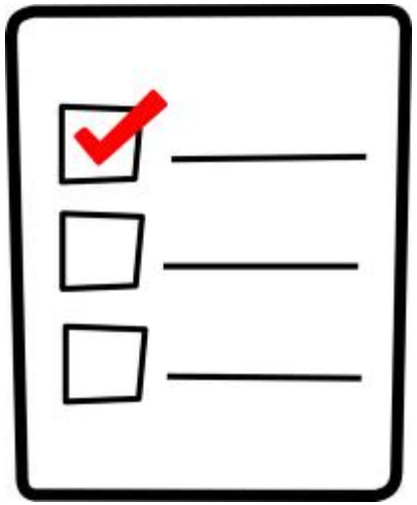
Presented by: **Tim Messman, Partner, Porter Keadle Moore**
Jim Rumph, Manager, Porter Keadle Moore

Porter Keadle Moore

CPAs | Advisors | www.pkm.com

Agenda

- Fraud
- Risk Factors
- Fraud Examples / Lessons Learned
- Information System Threats
- Fraud Examples / Lessons Learned
- Questions



Homecoming Queen

Homecoming Queen

Homecoming Queen

- Worked as accountant for a golf products company
- Arrested for stealing $800,000+ over a 16 month period
- She was a CPA and licensed real estate appraiser
- She obtained a debit card on the business account
- 54 unauthorized wire transfers - $358,885
  - $269,535 wired to businesses where she was an officer / registered agent
- 60 unauthorized debit card purchases - $411,387
- Serving 6 year sentence for grand theft

- Lessons Learned – Customer Training, Fraud Monitoring

Fraud

- Error vs. Fraud
- Focus on two types of fraud:
  - Fraudulent Financial Reporting – “Cooking the Books”
  - Misappropriation of Assets – Theft

Polling Question #1

- **Who is primarily responsible for preventing fraud?**
  - A) Board of Directors
  - B) Management
  - C) Auditors
  - D) A & B
  - E) A, B & C

Who is Primarily Responsible for Preventing Fraud?

- FDIC - The primary responsibility to prevent fraud and insider abuse rests with the **board of directors and senior management**. To properly execute their fiduciary duties, management must implement internal controls and other safeguards to prevent fraud and theft whether internally or externally perpetrated.

- Fraud Prevention

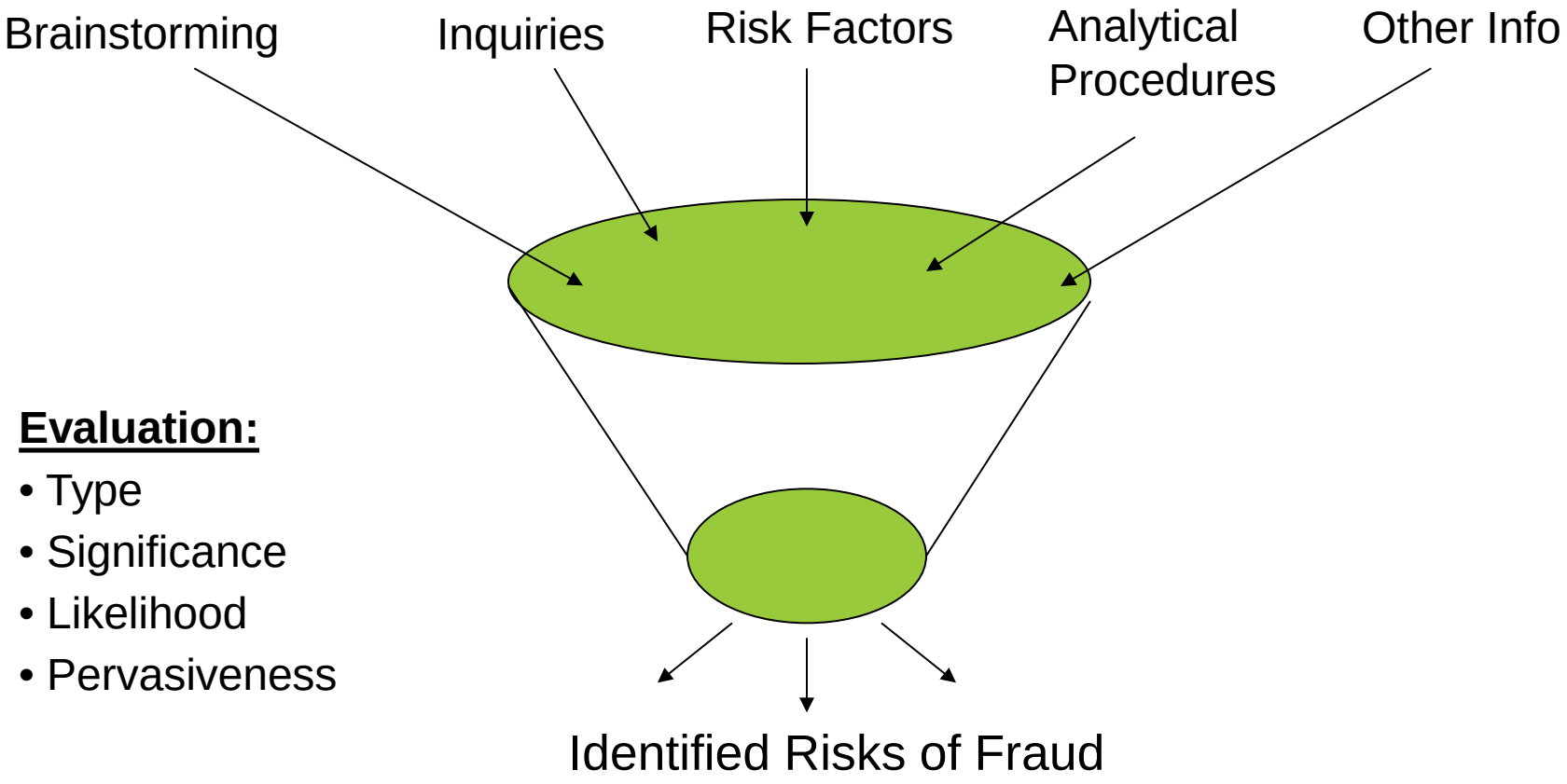
- Fraud Detection

Fraud Prevention / Detection

- Tone at the Top
- Training
- Risk Assessment
- Properly Designed Controls
- Properly Operating Controls
- System for Oversight of Controls
- Whistleblower
- Prosecute, Prosecute, Prosecute!

Identifying Fraud Risks

Sources of Information



Evaluation:

- Type
- Significance
- Likelihood
- Pervasiveness

The Fraud Triangle

Polling Question #2

- **Have you had a fraud occurrence at your institution? (fraudulent financial reporting or misappropriation of assets)**
  - A) Yes
  - B) No
  - C) I plead the Fifth

Risk Factor Examples
Misappropriation of Assets

▲ Incentives and Pressures

- Adverse relationships between the entity and employees
- Personal financial obligations may create pressure on management or employees

Payday Loan

- CFO under financial duress
- No segregation of duties over payroll process
- Posted payroll for himself 1 week early
- No loss to the bank
- CFO Fired

- Lessons Learned – segregate duties, if possible, or add other mitigating control (review)

Risk Factor Examples
Misappropriation of Assets

▲ Opportunities

- Large amounts of cash on hand
- Inadequate internal control over assets

Sick Teller

- Teller managed detached drive thru location for 15 years
- Never took vacation
- Sick one day
- $60,000 loss
- Surprise cash counts did not include drive thru location

- Lesson Learned – mandatory vacation policy, every teller subject to surprise cash counts

What Cash???

- Tellers accepted delivery of cash from armed courier
- Signed for 2 bags
- Verified funds later and only had 1 bag
- $100,000 loss

- Lesson Learned – teller training, ensure procedures require verification of cash

Fictitious Loans

- Loan Officer made fictitious unsecured loans
- No segregation of duties over lending
- $130,000 loss

- Lesson Learned – segregate duties, review of employee accounts

Time Deposit Shell Game

- 20+ year customer service representative lapped CD's from one customer to another
- Lack of segregation of duties and controls over opening and closing accounts
- $100,000+ loss
- Lesson Learned – mandatory vacation policy, segregate duties, review of employee accounts

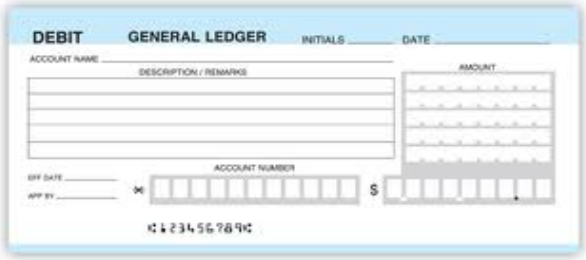
Risk Factor Examples
Misappropriation of Assets

▲ Attitudes and Rationalizations

- Behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee
- Tolerance of petty theft

GL Tickets

- Bank employee used general ledger tickets to credit her personal account
- G/L tickets did not require dual sign-off
- Amounts were small enough that it did not get caught in the budget to actual analysis
- $22,000 loss over 3 year period



- Lesson Learned – dual sign-off of G/L tickets, system control to prevent entries between misc expense accounts and deposit accounts, review of employee deposit accounts

New Account Fraud

- Bank customer used CPA to manage funds
- CPA opened another account for customer (unauthorized)
- Stole over $1 million over 10 year period
- Lesson Learned - employee training, customer training

Polling Question #3

- **What percentage of cyber attacks are aimed at small businesses (1-250 employees)?**
  - A) 10%
  - B) 30%
  - C) 70%

Why is this Important?

30% of all cyber attacks target business with fewer than 250 employees

- **Targeted attacks are growing the most among businesses with fewer than 250 employees. Small businesses are now the target of 31 percent of all attacks, a threefold increase from 2011.**
- **Most attacks were not difficult**
- **Cyber crime has surpassed illegal drug trafficking as a criminal moneymaker**

Source: Symantec Internet Security Threat Report

Prevention is Key!

Types of Threats to Information Systems

How do breaches occur?

- **52%** used some form of hacking (-)
- **76%** of network intrusions exploited weak or stolen credentials (-)
- **40%** incorporated malware (-)
- **35%** involved physical attacks (+)
- **29%** leveraged social tactics (+)
- **13%** resulted from privilege misuse and abuse

- ▲ Physical
- ▲ Social Engineering
- ▲ Malware/Virus

What commonalities exist?

- **75%** driven by financial motives (-)
- **71%** targeted user devices (+)
- **54%** compromised servers (-)
- **75%** are considered opportunistic attacks (-)
- **78%** of initial intrusions rated as low difficulty
- **69%** discovered by external parties
- **66%** took months or more to discover (+)

Source: Verizon Data Breach Report

Physical Threats

- Dumpster Diving
- Lost backup tapes
- Information that can be used in social engineering attacks

Dumpster Diving at McAlister's Deli

- Restaurant discarded job applications with sensitive information including Social Security numbers

- Over $60K in identify theft fraud occurred as a result

- Lessons Learned - Educate employees on safe disposal of customer information

Social Engineering

▲Types of Exploits:

- Phishing through emails
- Phone Calls
- USB devices
- Wireless
- Spoofing

▲ Preying on the Best Qualities of Human Nature:

- The desire to be helpful
- The tendency to trust people
- The fear of getting into trouble

Phishing

- Phishing emails were sent to client base of a small community bank
- Email asked users to call in to verify their account numbers
- Lessons Learned – Customer Education, Purchase similar domain names

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Malware Threats

- Malware: Short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent.

- Malware includes any type of virus, trojan, spyware or other malicious software intended to gather sensitive information, gain access, or disrupt operations

Nobody's Listening

- A Bank had a $750K wire transfer fraud
- Customer computer was compromised by malware
- Customer ignored out-of-band alerts – alerts were sent to the "wrong" person (the owner)
- Lessons Learned – Preventative controls, customer training

Multifactor Authentication Letdown

- Our client was using multifactor authentication using RSA keys that flashed a one-time password every 30 seconds for cash management customers
- A hacker “tailgated” the one-time password and sent a fraudulent ACH transaction
- The client assumed that the wire was legitimate because of the RSA controls
- Lessons Learned – Customer education, controls are not foolproof, always room for improvement

Polling Question #4

- **What is the name of the recently discovered vulnerability that affects OpenSSL and allows passwords to be stolen?**
  - A) Heart Attack
  - B) Heartbleed
  - C) SSL Hacker
  - D) None of the above

Heartbleed Bug

IE Zero Day Vulnerability

Lessons Learned

- People are your first line of defense
  - Train them well!
- Can’t Outsource Responsibility!
- Prevention of attacks is far cheaper than responses to attacks.
- Always use a layered security approach

Questions

Contact Information

- **Tim Messman, Audit Partner**

  (404) 420-5797

  tmessman@pkm.com

- **Jim Rumph, Systems Manager**

  (404) 420-5639

  jrumph@pkm.com

Sign up for our Next Webinar!

- Recent Tax Developments in Banking
  - June 25, 2014 3:00 - 4:00pm (EST)

http://www.pkm.com/events/cfo-roundtable/