



Fraud Risk Assessment and Management

Presented by

Greg Depue, *Senior Manager*, Capin Crouse LLP

Balloon Boy! Fraud or Hoax?



What is fraud?

In the broadest sense fraud is:

- An intentional deception
- Made for personal / unfair gain or to damage another individual
- It is a crime and also a civil law violation (varies by jurisdiction)
- Many hoaxes are fraudulent, not made for personal gain – not technically frauds (also frauds in art, science, archeology, etc.)

Per the ACFE (Association of Certified Fraud Examiners) –

- Fraud is *“The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”*

What is Fraud? - continued

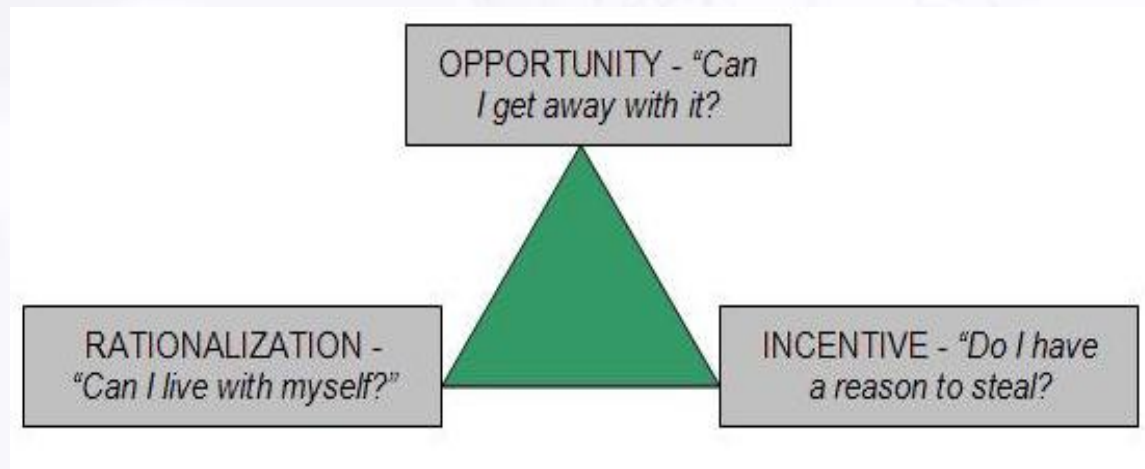
- Fraud encompasses an array of irregularities and illegal acts characterized by intentional deception. The five elements of fraud are:
 - A representation about a material fact, which is false,
 - And made intentionally, knowingly, or recklessly,
 - Which is believed,
 - And acted upon by the victim,
 - To the victim's damage.

What is Fraud? - continued

- Fraud, like other crime, can best be explained by three factors:
 - 1) A supply of motivated offenders;
 - 2) The availability of suitable targets;
 - 3) The absence of capable guardians or a control system to “mind the store”

Fraud Triangle

- perceived opportunity
- incentive / pressure or need
- attitude / rationalization



Fraud Triangle - continued

- There are four elements that must be present for a person or employee to commit fraud – fueled by the need, greed, incentive or pressure - (another perspective on the “Fraud Triangle”) -
 - Opportunity
 - Low chance of getting caught
 - Rationalization in the fraudsters mind
 - Justification that results from the rationalization

Workforce Adjustment?

Has your organization had to do a layoff or furlough staff due to the current state of the economy? A layoff or similar workforce reduction situation is a quick way to introduce elements of the fraud triangle that didn't previously exist. Consider the following before and after scenarios:

	<u>Before Layoff</u>	<u>After Layoff</u>
OPPORTUNITY	Plenty of checks and balances in place	Less people involved in the process
INCENTIVE	No pressure to steal from organization	Unstable economy is affecting investments, family members, etc.
RATIONALIZATION	Happy employees, cohesive workplace, Extremely loyal to organization	Angry and/or scared employees, Less loyalty to organization

Insider Issues – Fraud Magazine – Vol 23. No. 5, Sept / Oct 2009

- The level of fraud has increased since the beginning of the economic crisis.
- Current increase comes from intense pressure faced by many individuals
- Loyal employees are under pressure (what kind of pressure?)
- Employees pose the greatest fraud threat in the current economy
- Layoffs are affecting organizations' internal control systems
- Fraud levels are expected to continue rising
- Organizations need to take seriously the threat posed by employees
- Fraud thrives in times of economic turmoil
- However - even while facing budget reductions, companies have not cut spending on fraud-related internal controls

Fraud - Attributes & Elements

- Acts are unknown, unseen – clandestine
- Committed by a person or persons in violation of their duties to the NPO (violation of fiduciary duties or responsibilities)
- Purpose - directly or indirectly benefiting the perpetrator (or to bring harm to the NPO – vengeance)
- Causes financial harm or injury to the NPO – its assets, revenues, reserves, reputation, existence, etc.
- Misappropriation, manipulation of financial information, corrupt purposes & practices

– continued

Fraud - Attributes & Elements, continued

- White Collar Crime –has come to be a generic term for a broad & ever expanding range of non-violent criminal activity including but not limited to: embezzlement, bribery, money laundering, illegal lobbying activities, consumer fraud, price fixing, income tax fraud, and computer "hacking" or computer break-ins.
- KPMG Australia national head of forensics Gary Gill says the numbers are significant, and he suggests only about 50% to 60% of all frauds are reported, and only a fraction of those end up in court.

Fraud – factors to consider

- Ponzi / pyramid schemes – more common than you think – mostly on a small scale – “too good to pass up” – I’m not greedy!
- Current, slow economy (recession)
- Attitude - management doesn’t want to admit fraud is possible – not in MY Christian ministry!
- Not “fraud savvy” – no fraud risk assessment, poor internal controls, no process or function responsible for assessing and monitoring risk – do you offer an “open door”?
- Poor, slow or inadequate internal financial reporting
- A fraud has been committed and discovered! (usually the hard way) – now what? What do I do?

Fraud – factors, continued

Financial Statement Fraud:

- A need to alter reports of financial performance (for better or worse):
 - Noticeable, unexpected difference – from projections (even in the current economy)
 - Does not track with budget
 - Major changes from prior period or prior year
 - Why? What is the motivation? – fund raising, banks, government, watch-dog groups, etc.

Fraud factors, continued

- Management can easily override established internal controls, or:
 - Is compensation or recognition tied to performance?
 - Is management dominated by a single person or group?
 - Does management display significant disregard for regulations & controls?
 - Has management restricted auditor (internal / external) access to documents or personnel?
 - Has management / board set unrealistic financial goals?
 - Is there a past history of illegal or unethical conduct?

Fraud factors, continued

- Who is likely to commit fraud?
 - Older employee – trusted, responsible, solid worker
 - Stressed out employee
 - Disgruntled employee
 - Employees living above their means
 - Employees who never take a vacation
 - Employees who are unnaturally compulsive about their jobs / overly diligent, may frequently work nights and weekends
 - Employees experiencing financial difficulties or emergencies
 - Employees with addictions (drugs, alcohol, gambling, other vices)

Fraud factors, continued

- Window of Opportunity –
 - Weak internal controls
 - Too much trust – usually in one key person
 - Poor management oversight
 - Lack of financial audit (external and internal)
 - No background checks on key employees
 - Lack of independent check / reconciliation and review of bank statements and credit card statements
 - Failure to take advantage of bank Positive Pay service
 - Failure to take advantage of bank lock box or caging service
 - After auditors conclude their field work for one year and before they return to start their field work for the next year.
 - Nepotism

Fraud Factors, continued

- “Check 21” - easier for fraud to be perpetrated and harder to detect – harder to audit
- Weak computer / internet security - fraud (internal & external – offline and online); IT department, gate keepers, hackers, viruses, Trojan viruses, and phishing
 - Online banking users – vulnerabilities
 - Identity Theft – what information do you keep on your computers? (personal identity, medical identity, etc.) (HIPPA)
- Insiders & outsiders – may be working together, collusion
- Weak purchasing system - procurement fraud

Fraud Factors, continued

- NPO's – 4 consistently risky areas
 - Incoming funds (checks and cash); donations, memberships, revenue, etc.
 - Printing, advertising and consulting expenses
 - Postage expenses
 - Personnel related expenses – wages, payroll taxes, employee fringe benefits (including credit cards and expense reimbursements) – “Most commonly payroll or accounts payable functions were the most susceptible to accounting fraud, usually by the creation of fictitious payments.”

Case Study 1

- Payroll Clerk
 - worked in the ministry for over 10 years
 - had held several other positions for ministry, trusted worker
 - payroll clerk for over 3 years, full-time, hourly worker
 - became single parent, financial hardships
 - able to enter & approve own payroll – hours worked & rate
 - increased hourly rate, entered over-time hours, double time, bonuses
 - controller did not carefully review work or payroll
 - fraud discovered by accident, controller compared payroll expense to budget at end of year and found overpayments

Case Study 2

- Small College VP of Finance
 - “One Man Show” – was on the regional accreditation team
 - approved & signed checks,
 - reconciled bank accounts, ran all reports, presented reports to the board,
 - had full access to all financial computer programs and data
 - no one reviewed or approved work, was highly respected & loved
 - never closed the books – always made an “opening journal entry”
 - former external auditors never questioned controls or processes,
 - used college account to pay personal bills & credit cards, mortgage, vacations
 - college rented VP’s house – house was purchased with college funds
 - new external audit firm came in and uncovered the fraud

Who commits most of the fraud?

- Male bosses / managers (long-serving male executives) (middle aged, male, senior executives) – 60% of all fraud – over half of them actually committed over 20 separate offenses– according to April 2007 BBC survey – “Status or position in the company makes it easier for them to bypass internal controls and inflict greater damage on the company,”. As for the scale of losses, among the cases examined, the average fraud was 1m Euros (\$1.4m; £680,000) – similar findings in Australia and US.
- Small companies – most vulnerable, easier for one person
- Staff members – up to 30% of business fraud
- Many are first-time offenders – may be trying to “beat the system” (or it may be a game)

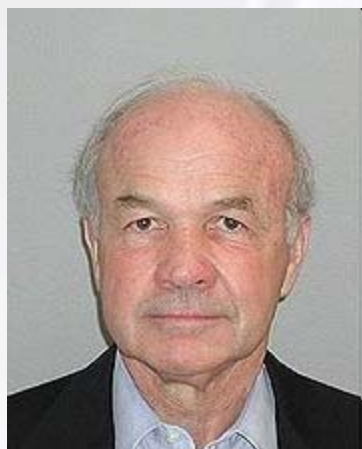
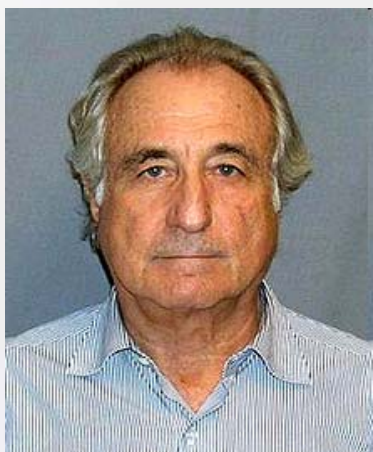
Recent & Historical Fraud Schemes

- ENRON – financial statement fraud – Ken Lay, Jeffrey Skilling
- World Com – financial statement fraud – Bernie Ebbers
- HealthSouth – financial statement fraud – Charles Scrushy
- Madoff – Ponzi – sentenced and in prison (150 years and he is 71)
- Michael Riolo – Boca Raton, FL– sentenced 10/16/09 –\$44M Ponzi
- Gordon Grigg – Tennessee financial advisor – TARP related Ponzi – invest in debt backed by federal gov. bailout program -\$10.9M – April 2009
- Foundation for New Era Philanthropy (1989 – 1995) – Ponzi \$500M – (exposed by college professor) – John G. Bennett Jr.
- DTS – CFO – shell companies, forgery -\$165K
- Lakewood Church & School, Marion, IN – Dir of Finance - \$276K
- Former pastor & sons – Indiana – securities fraud - bonds \$120M –
- Arizona Baptist Foundation - \$585M, Ponzi & shell companies, 1999

Recent & Historical Fraud Schemes, continued

- Cornell Univ. – 5 year, \$23M grant, research never happened, \$4.4M paid in settlement – exposed by whistleblower
- Univ. of California, Harvard, Mayo Clinic, etc. research grants – whistleblowers

Who are these people?



Case Study 3

- Mission organization VP of Finance
 - VP for over 5 years, good performance, valued / trusted by management
 - behind the scenes became tyrant to all in finance dept. – fear factor
 - no-one else went to upper management or board –
 - carried all checks to Pres / CEO for signature – always in a hurry to have checks signed right away –
 - ministry accounts used to purchased furnishings & improvements for home, pay personal credit cards, vacations, purchase personal vehicle
 - paid family members to make home improvements
 - renting ministry property to others for cash & pocketing cash
 - opened bank secret accounts, transferred mission funds to them
 - whistleblower came forward and called external audit manager

Other Types of Fraud

- Medical/insurance claims fraud
 - Other insurance claim fraud (liability, workers comp, false property & casualty claims, etc.
 - Medicaid / Medicare scams and false medical claims by employees with self-insured plans
 - Billing for inappropriate or unnecessary procedures
 - “Up Coding” and billing for complex services when only simple services were performed

Financial Statement Fraud

- False financial statements – data and reporting manipulation (least frequent, most \$)
 - Overstatement of revenue
 - Fictitious revenue
 - Understatement of expenses
 - Overstatement of assets
 - Understatement of liabilities
 - others

Fraud Opportunities

- Conflict of interest fraud - possibly collusion or corruption: using position of influence and receiving help; extortion, bribery (in the middle for frequency, relatively small \$)
- Misappropriation of Assets – (most frequent, smallest in \$) cash: skimming, larceny, kiting,
 - Mailroom larceny, unrecorded sales, stolen donations
- Credit card fraud – fictitious refunds, personal purchases
- Fraudulent EFT / ACH bank transfers

Opportunities, continued

- Check fraud
 - Expense fraud - missing documents – destruction of records, padding / inflating, double billing,
 - Paying personal bills / personal purchases
 - Reimbursement fraud (expense account abuse)
 - Manually prepared checks vs. computer prepared / check fraud / altered checks / missing checks, etc.
 - Other check doctoring schemes

Opportunities, continued

- Payroll fraud –
 - Expensing “Phantom Employees” or padding hours worked
- Diversion of assets / theft
 - Inventory, office décor, donated inventory, etc.
- Bid rigging and price fixing
- Journal entry fraud – (as a cover up for or to initiate other fraudulent activities)
- Bribery & Corruption – fictitious bills, family, kickbacks

Opportunities, continued

- Purchases and appropriations for personal use
 - Use of ministry property for personal purposes
 - Cars, cell phones, computers, copy machines, etc.
 - Ministry employees paid by ministry for personal work – remodeling, maintenance, construction, etc.
 - “loan” of company equipment with a cash “gratuity” paid to employee
 - personal work done on ministry time and at ministry expense

Opportunities, continued

- Procurement Fraud - Purchase order or purchase department –
 - False invoices - “Phantom Billing” for services that are not performed, or products not delivered
 - Fictitious vendors, customers or orders –
 - Overcharging for items actually purchased for much less.
 - Billing for new equipment but providing used equipment
 - Billing for expensive equipment but providing low-cost equipment.
 - Charging for equipment or supplies that were never ordered
 - “Double Billing” by charging more than once for the same service.
 - Billing for brand-named supplies when generic were provided
 - Kickbacks

Case Study 4

- Accounting Clerk

- ministry employee for over 20 years – in finance department
- primary responsibility - employee benefits / self insured med program, section 125 plan, etc.
- able to write & sign checks on the various bank accounts, prepare & post journal entries, reconcile bank accounts associated with benefit programs – presented reports to CFO who did a cursory review
- no detailed management review or approval of the activities, files, paid bills, etc.
- made payments for personal expenditures for over 5 years before external auditors noted the fraud – large \$ fraud
- able to “cover tracks” / conceal the fraud through journal entries

Employment Fraud

- Résumé fraud – or *application fraud* refers to any act that involves providing fictitious, exaggerated, or otherwise misleading information on a job application or résumé in hopes of persuading a potential employer to hire an applicant for a job they may be unqualified for, or that they are less qualified than other applicants (or hiding a criminal history)
- Job fraud - fraudulent or deceptive activity or representation on the part of an employee or prospective employee toward an employer

More Fraud

- Grant fraud - Univ prof - Dept of Ed grant fraud – federal research grants, TARP, bail out funds, etc. – FEMA fraud,
- Ponzi scheme – pyramid schemes – Madoff, Riollo, Grigg
- Pyramid scheme – is a non-sustainable business model that involves the exchange of money primarily for enrolling other people into the scheme, often without any product or service being delivered.

How is fraud uncovered or discovered?

- According to Edward J. McMillan – Preventing Fraud in Nonprofit Organizations
 - Whistle blower – 30%
 - Internal audit / Program specific audit – 18%
 - **Accidentally – sheer luck – 50% of all frauds are discovered this way**
 - External audit – 2%

Strengthen Operations to Resist, Detect and Possibly Prevent Fraud

- Setting the “*tone at the top*” – the highest standards
 - Creating a positive environment
 - Developing a *code of conduct* – fraud policy statement
 - Having fair and balanced discipline – *policy manual* for board & employees – communicate well & follow through
 - Improve monitoring of *conflict of interest* statements – ensure they are filed and are correct; sanctions for conflict of interest are enforced
 - Fraud *whistleblower* program (possibly a reward program) (“fraud hotline” – trusted, safe & confidential) – “Clear policies for whistle-blowing will stop a lot of these events occurring early.”

Prevent Fraud – Strengthen Defenses Against Fraud

- Having a strong and independent, inquisitive *audit committee*
 - Identifying and measuring fraud risks (COSO framework) – with continuous monitoring
- Use an *internal auditor*
 - Hiring effective internal auditors and *Certified Fraud Examiners*
 - audits of regional and foreign offices
- Contracting capable & knowledgeable *external auditors*
 - Do they know you and your type of ministry, and are they trusted advisors? Good reputation? They can be a good resource.
 - Fraud inquiries conducted during an audit – resistance & reluctance by the ministry (information gathering - not accusation)

Prevent Fraud, continued

- Hiring and promoting the “right” employees (skills, attitude, ethics)
 - **Strict employment guidelines** – including background checks, criminal, credit, references, driving record, education and degrees attained, professional credentials, drug testing, FBI finger print check, etc. (check with your HR director and legal counsel on what is and is not permissible in your state)
 - **Increase training** for managers and those responsible for budgets and spending or institute continuous training (fraud skills & awareness training)
 - **Complete conditions of employment agreement** / employee manual – signed by employee, authorizing periodic inspection of employee offices, desks, lockers and personal areas – employee conduct statements (periodic / annual sign off)
 - "When you take on a new employee, make sure you screen them properly, and make sure you know what they have done in previous jobs because people who commit fraud usually have a history." Per KPMG study in Australia

Prevent Fraud, continued

- Combating fraud is a *team effort* – not just finance
 - Create *effective policies & procedures – internal controls!*
 - *Ask* “What could go wrong?” “Where could it happen?”
 “When?” “How?” “Who?” – *learn to think like a fraudster* – identify the risks – consider asking each employee “Do you suspect any fraud within our organization?”
 - *Whistleblower policy* – tell managers / workers - expectations & how (their role) – protect the whistleblower!
 - *Early detection* – create awareness & **fear** – publicize efforts and results
 - *Competent employees* – paying attention to details – high integrity
 - *Educate employees*

– continued

Prevent Fraud, continued

- ***Better oversight*** of department chairpersons or directors – look for management exceptions or overrides of policy & procedures
 - ***Separation or segregation of duties*** – with appropriate oversight
 - ***Periodic review*** of large expenditures or income, grants / awards (note: both received or expended) (also false agency transactions)
 - ***Program audits*** – ensure reports are correctly and completely filed; and reviewed
 - ***Improve controls*** over expenditures – especially credit cards and debit cards
 - ***Standardizing and streamlining processes*** – simpler is better
- continued

Prevent Fraud, continued

- ***Secure check stock and signature stamps***, etc. (if computer checks – software and hardware security)
- ***Confirm*** amount of activity with ***large vendors*** – internal audit, validate vendor listing
- ***Dual signatures*** on large \$ checks and on ALL wire transfers, EFT, ACH activity (safeguards on automated check signing)
- ***Employee bonding*** / fidelity bond (employee dishonesty insurance) – protects against internal embezzlement
- If very small staff – consider volunteers or board members helping out in key roles -

– continued

Prevent Fraud, continued

- Conduct *surprise “visits”* – usually internal or external auditors, but can be management
 - Surprise *petty cash count*
 - Bank and credit account “cut off” statements – *review bank reconciliations* – *review payroll and payroll reconciliations*
 - *Surprise transaction tests* – income and expense
 - *Surprise visit* to mail room or counting room – maybe install cameras
 - *Surprise inspection* of HR files – review all current employee files & get a list of all current employees on payroll – focus on new employees – review employee benefits withheld and paid
 - *Surprise payroll review* – compare HR list above to payroll
- continued

Prevent Fraud, continued

- Strengthen computer and internet security – firewalls & adherence to good practices
 - ***Backup*** computer files and keep several generations and annual back ups (kept in ***secure, offsite, limited access location***)
 - Set up appropriate ***levels of computer security*** on all finance related software and computers
 - ***Change computer passwords*** on a regular basis (require this for all employees for all computer access and financial software access) keep passwords in safe location monitored by a person who has no financial or accounting activities (***strong / complex passwords***)
 - ***Monitor internet access*** – block questionable sites
 - Limit gateways into your system
 - ***Isolate e-mail servers*** from financial programs and data (separate servers)
 - Conduct a computer security “audit” – ***IT audit***

Preventing Fraud - A Check Signer's Responsibilities

1. Be sure that backup documentation is attached to support the check.
2. Review this documentation and compare to the check:
 - Amount agrees? Vendor name agrees? Dates look correct?
3. Review the documentation to ensure that it is a reasonable and expected business expense and that it is supportive of your overall mission:
 - Does the support show the required approvals?
 - If you use purchase orders, is an approved purchase order also attached?
 - If the invoice is for physical items, is the delivery address the same as the business address?
 - If the invoice is for services, does the amount agree to any contracts that may relate to the service? Does the invoice clearly state the services being provided?

• continued

Preventing Fraud - A Check Signer's Responsibilities

- Are there original receipts to support expense reimbursements? Do expense reimbursements charges look reasonable and were they properly approved?
 - Does the backup look legitimate?
4. Ensure that the supporting documentation includes the *original* invoice, and not a copy. There should be a company policy on this to prevent duplication. (international staff – missionaries in 3rd world countries?)
 5. Also, ensure that the supporting documentation is an *invoice*, and not a monthly statement. There should also be a company policy on this.
 6. If you are not familiar with the vendor or the charges, go a few steps further in your review...make inquiries, ask for additional backup, talk to others involved, etc. Do what you need to do to ensure that the charges are legitimate. Don't automatically trust the response from the person who generated the check.

Red Flags of Ponzi Schemes:

You are in need of a better return on your investments?

Beware!

- Sounds Too Good to Be True
- Promises of Low Risk or High Returns
- History of Consistent Returns
- High-Pressure Sales Tactics
- Pressure to Reinvest
- Complex Trading Strategies
- Lack of Transparency
- Lack of Segregation / Separation – “one man show”, be concerned about any financial managers who manage, administer, and retain custody of the fund in question because the opportunity for fraud is high in these situations

Ponzi Schemes – fighting back

- Tips to keep the scammers away:
 - Ask questions—lots of them. Know who you are dealing with
 - Check credentials – know your vendors / suppliers / trusted advisors
 - Don't be greedy.
 - Seek professional or informed second opinions.
 - When evaluating an offer, always start your pro and con list with the "cons."
 - As with all investments, exercise due diligence in selecting investments and the people with whom you invest.
 - Make sure you fully understand the investment before you invest your money

What to do when you suspect fraud -

- Contact your CPA - don't try a do-it-yourself investigation
- Consider contacting a CFE and your Audit Committee:
 - Protecting evidence - gathering data and documentation - facts
 - Identifying clues or badges of fraud, who is involved – collusion?
 - Conducting interviews – don't squander the opportunity
 - Let's the owners / managers get back to the ministry / business
- Review policies and procedures – identify weak areas / controls
- Be discrete in your inquiries – don't discuss this around the office
- If your suspicions appear to be supported by your inquiry what next?
- Never accuse anyone of impropriety – there must be proof

What to do when you discover fraud -

- Initiate an investigation – assemble a fraud team – don't hesitate!
 - Contact your attorney - follow instructions - call your CPA & CFE
 - There must be proof – must demonstrate fraud has occurred
 - Intent, misrepresentation, reliance, loss – document the facts
 - Qualify and quantify the loss
 - Work from copies (keep originals safe), take detailed & copious notes;
 - Review your insurance / fidelity bond – what does it require? Police report? Time frame to file claim? Collection of evidence?
 - Identify the perpetrator(s) – review employment agreement / policy, always have a witness at termination (before or after business hours?); protect yourself and other employees, ensure surrender of org. property, escort employee from office – employee does NOT collect his property - co-workers help
 - Stop the Loss - lock down the computer – pull the plug / don't turn it on, change passwords, limit remote access, secure physical files, protect evidence

What to do when you **discover** fraud - continued

- Ask - What safeguards / controls must be installed now?
- Deal with the perpetrator(s) – follow advice of attorney - police? prosecute? implement Biblical discipline?
- Consider – adverse publicity, legal costs, ministry morale,
 - What is the attitude of the offender
 - What part did the ministry play in this – culpability? poor internal controls?
 - Size of the loss
 - What publicity, if any, has already resulted?
 - Ministry, organization, church, denominational policy
 - Biblical / doctrinal position or teaching
 - What have you learned?



Thank you -

*Greg Depue, CFE, CPA
Capin Crouse LLP*

*1255 Lakes Parkway, Suite 130
Lawrenceville, GA 30043
gdepue@capincrouse.com*

