



# How to Protect Your Practice from Embezzlement & Fraud!

---



Medical Group Management Association

Central Florida, Fla.

# Speaker #1 Bio

WHO:	Jeff Holt, VP
PHONE:	W# 352-385-3800 / C# 810-441-1234
PROFESSION:	Senior Healthcare Business Banker for PNC Bank.
TENURE:	With PNC Bank for over 29 years. Over 9 years only servicing Healthcare Practices.
RESPONSIBILITIES:	Support Medical, Dental, and Veterinary practices by – * Revenue Cycle Review and Enhancement. * Practice Transition Support with Specialized Lending and Healthcare Banking Services. * Solution Resource with my Healthcare Business Professionals Partners.
COVERAGE AREA:	West Central Florida (Orlando area to the Gainesville area)
EDUCATION:	University of Michigan - Bachelors of Business Admin Certified Medical Practice Executive (CMPE) with the American College of Medical Practice Executives (ACMPE) in process. (1 test down and 1 to go!)

# Speaker #2 Bio

WHO: Yung Nguyen  
PHONE: (813) 221-6145  
PROFESSION: Healthcare Treasury Management Officer for PNC Bank  
TENURE: 13 years in Financial Services  
9 months with PNC Bank  
RESPONSIBILITIES: Supports Medical, Dental, and Veterinary practices by –  
\* Improving AR Collections  
\* Implementing Information Reporting  
\* Offering Payment Solutions  
\* Reducing Fraud and Embezzlement  
COVERAGE AREA: West and Central Coast Florida  
EDUCATION: University of South Florida  
Bachelor Degree in Business Management

# How Likely is Embezzlement or Fraud to Happen?!

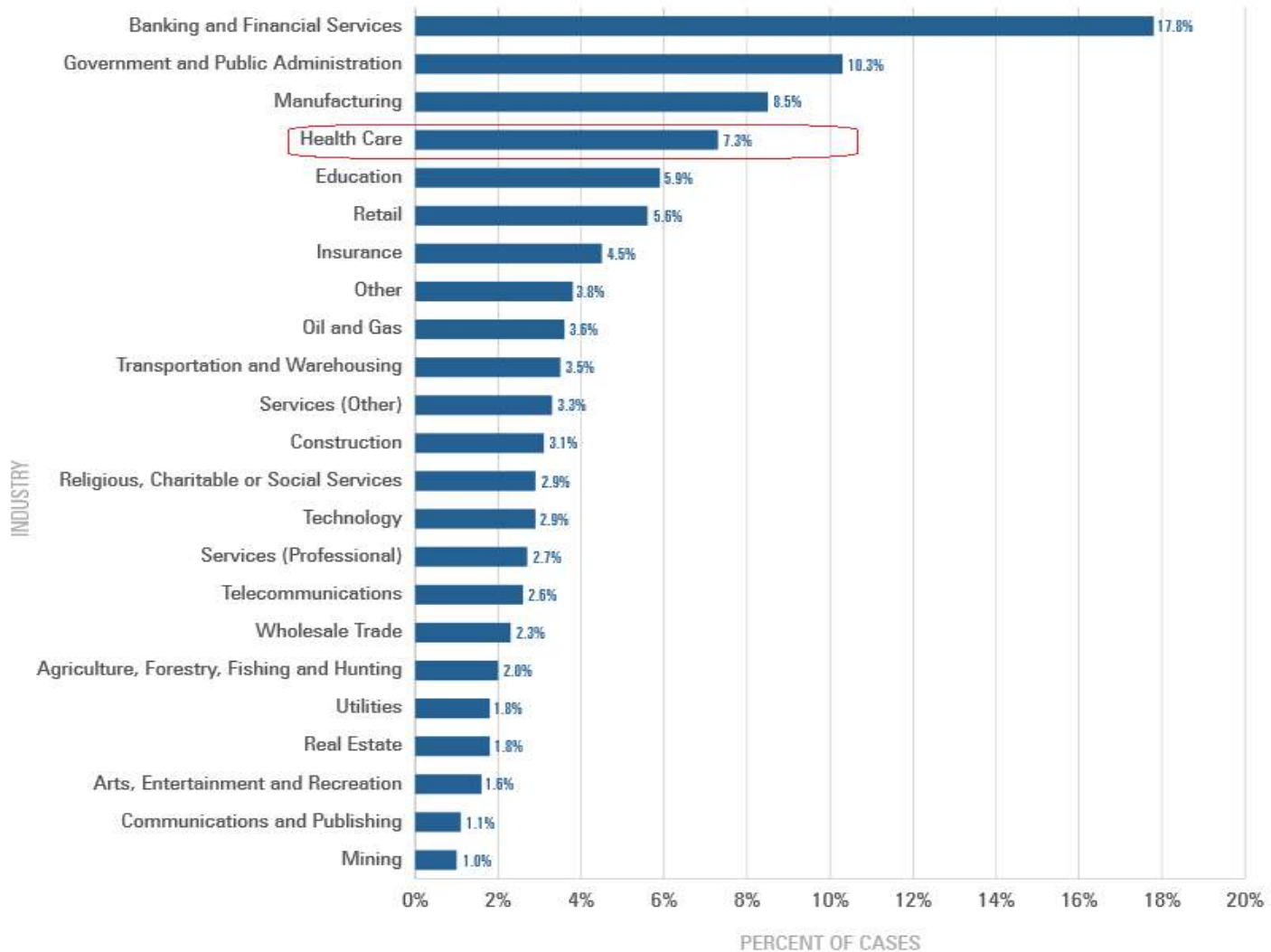
- ▶ Embezzlement strikes almost 60% of Healthcare Practices.(1)
- ▶ Medical & Dental practices lose \$25 billion annually.(2)
- ▶ The median loss for healthcare practices for 2014 was \$175,000.(2)
- ▶ Estimates are that each organization loses 5% of their revenue to fraud each year.(2)
- ▶ Small organizations are disproportionately victimized by occupational fraud. These organizations are typically lacking in anti-fraud controls compared to their larger counterparts, which makes them particularly vulnerable to fraud.(2)
- ▶ 86.6% of fraudsters have never been previously charged or convicted for a fraud-related offense as of 2014.(2)
- ▶ 81.7% of fraudsters have never been punished or terminated.(2)
- ▶ About 70% of embezzlement is a result of lack of enforced internal controls, and lack of management review.(2)
- ▶ **A MGMA survey reports “82% of respondents who had worked at a medical group that was victimized by employee theft or embezzlement.”(3)**

(1) David Harris of Prosperident

(2) Association of Certified Fraud Examiners (ACFE)

(3) MGMA Connections Magazine, September 2014

# Industry of Victim Organizations by Percent of Cases



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

# Industry of Victim Organizations by Median Loss

Industry	Number of Cases	Percent of Cases	Median Loss
Mining	13	1.0%	\$900,000
Real Estate	24	1.8%	\$555,000
Oil and Gas	49	3.6%	\$450,000
Wholesale Trade	31	2.3%	\$375,000
Technology	39	2.9%	\$250,000
Manufacturing	116	8.5%	\$250,000
Construction	43	3.1%	\$245,000
Agriculture, Forestry, Fishing and Hunting	28	2.0%	\$242,000
Transportation and Warehousing	48	3.5%	\$202,000
Banking and Financial Services	244	17.8%	\$200,000
Services (Professional)	37	2.7%	\$180,000
Health Care	100	7.3%	\$175,000
Arts, Entertainment and Recreation	22	1.6%	\$168,000
Other	52	3.8%	\$130,000
Services (Other)	45	3.3%	\$125,000
Telecommunications	36	2.6%	\$120,000
Utilities	25	1.8%	\$100,000
Insurance	62	4.5%	\$93,000
Religious, Charitable or Social Services	40	2.9%	\$80,000
Government and Public Administration	141	10.3%	\$64,000
Education	80	5.9%	\$58,000
Retail	77	5.6%	\$54,000
Communications and Publishing	15	1.1%	\$50,000

© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

# Frequency of Schemes Based on Industry

Industry/ Scheme	Banking and Financial Services	Government and Public Administration	Manufacturing	Health Care	Education	Retail	Insurance	Oil and Gas	Transportation and Warehousing	Services (Other)	Construction	Religious, Charitable or Social Services
Cases	244	141	116	100	80	77	62	49	48	45	43	40
Billing	5.7%	19.1%	22.4%	29.0%	33.8%	10.4%	17.7%	24.5%	33.3%	28.9%	34.9%	32.5%
Cash Larceny	13.1%	10.6%	6.0%	12.0%	6.3%	15.6%	6.5%	2.0%	2.1%	11.1%	14.0%	7.5%
Cash on Hand	18.9%	12.1%	7.8%	16.0%	16.3%	22.1%	1.6%	2.0%	10.4%	11.1%	7.0%	12.5%
Check Tampering	5.7%	5.7%	7.8%	21.0%	10.0%	7.8%	4.8%	4.1%	20.8%	17.8%	27.9%	35.0%
Corruption	37.3%	36.2%	54.3%	37.0%	36.3%	22.1%	33.9%	57.1%	29.2%	35.6%	46.5%	30.0%
Expense Reimbursements	4.1%	12.8%	7.8%	23.0%	31.3%	3.9%	4.8%	14.3%	14.6%	17.8%	27.9%	32.5%
Financial Statement Fraud	10.2%	5.0%	13.8%	8.0%	10.0%	6.5%	3.2%	12.2%	10.4%	6.7%	11.6%	7.5%
Non-Cash	13.1%	17.7%	34.5%	12.0%	12.5%	33.8%	12.9%	16.3%	33.3%	17.8%	20.9%	15.0%
Payroll	5.3%	15.6%	8.6%	15.0%	16.3%	5.2%	8.1%	6.1%	16.7%	6.7%	18.6%	20.0%
Register Disbursements	2.5%	0.7%	2.6%	3.0%	5.0%	13.0%	0.0%	0.0%	4.2%	6.7%	2.3%	2.5%
Skimming	5.7%	11.3%	4.3%	18.0%	20.0%	18.2%	22.6%	2.0%	6.3%	33.3%	7.0%	12.5%

© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

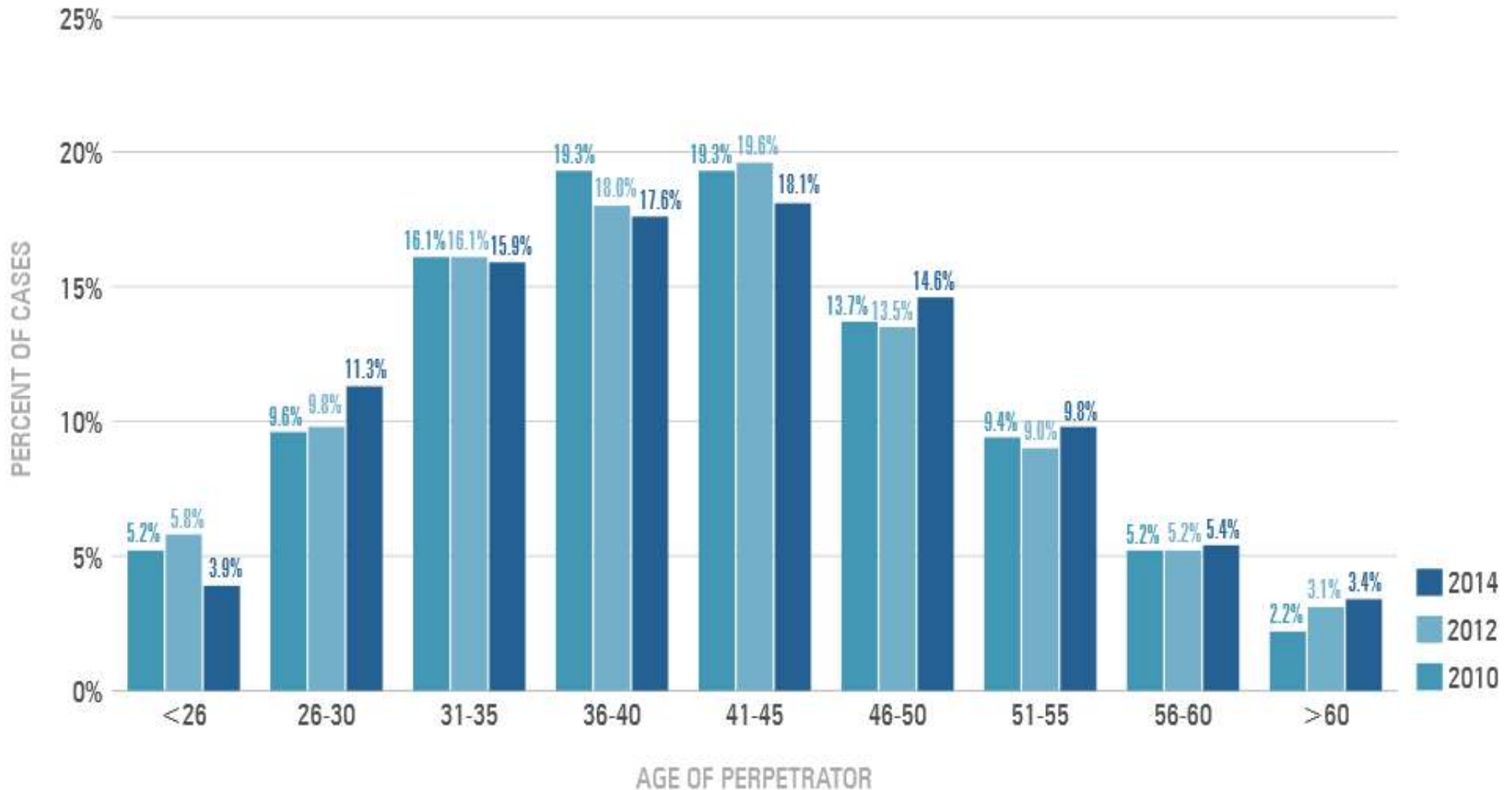


# Characteristics of Embezzlers

- ▶ Know “Who is the typical thief?”
  - A long time employee
  - Has the full trust of the doctor and is a devoted employee
  
- ▶ What characteristics should alert you?
  - This person never takes a vacation
  - They are very protective of their job
  - Work many hours of overtime, often alone
  - Never cross trains a substitute
  - The doctor often depends on this person in office emergencies
  - Usually living beyond their means
  - Lifestyle and behavioral changes

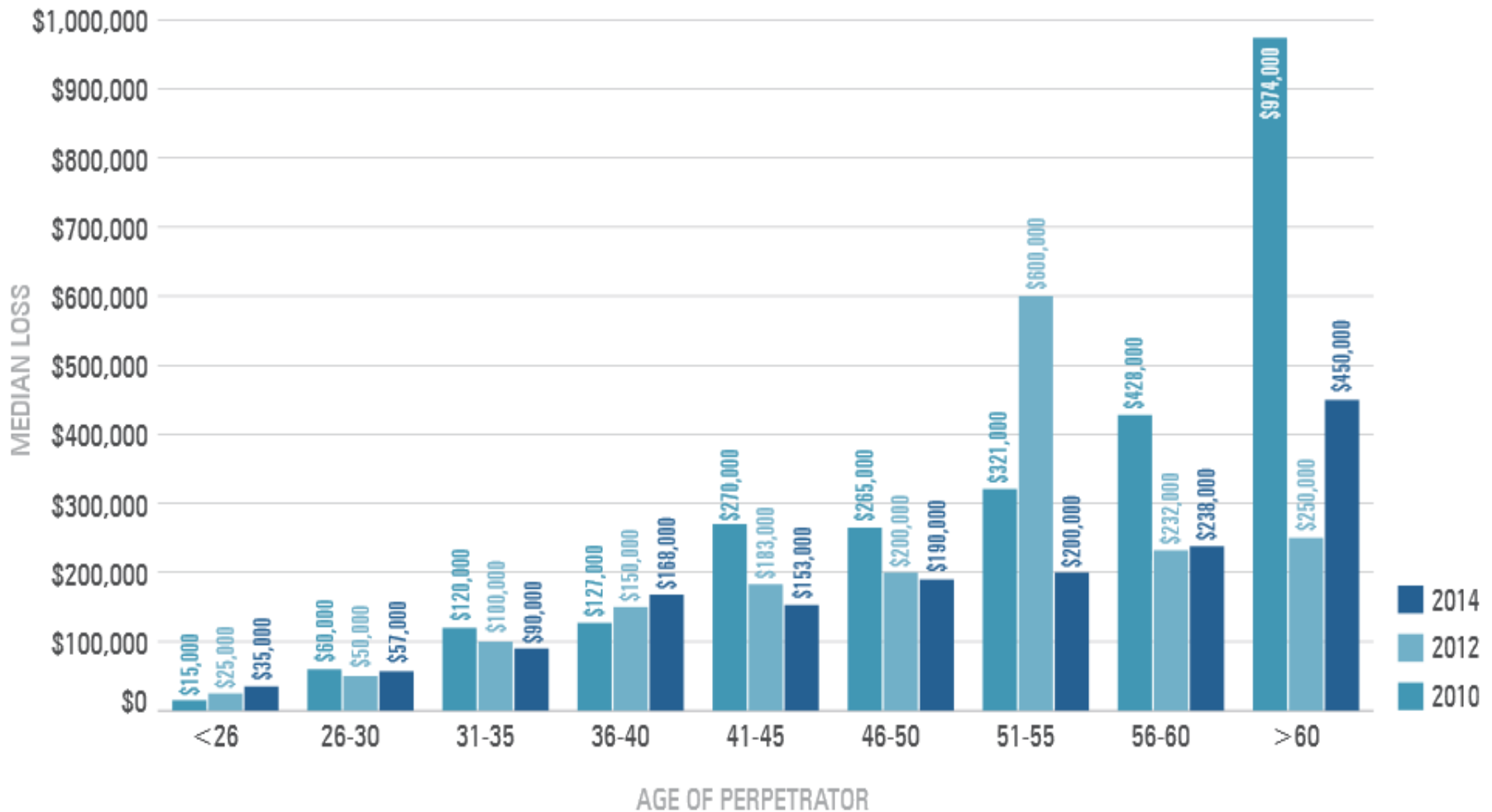


# What is the Typical Age?



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

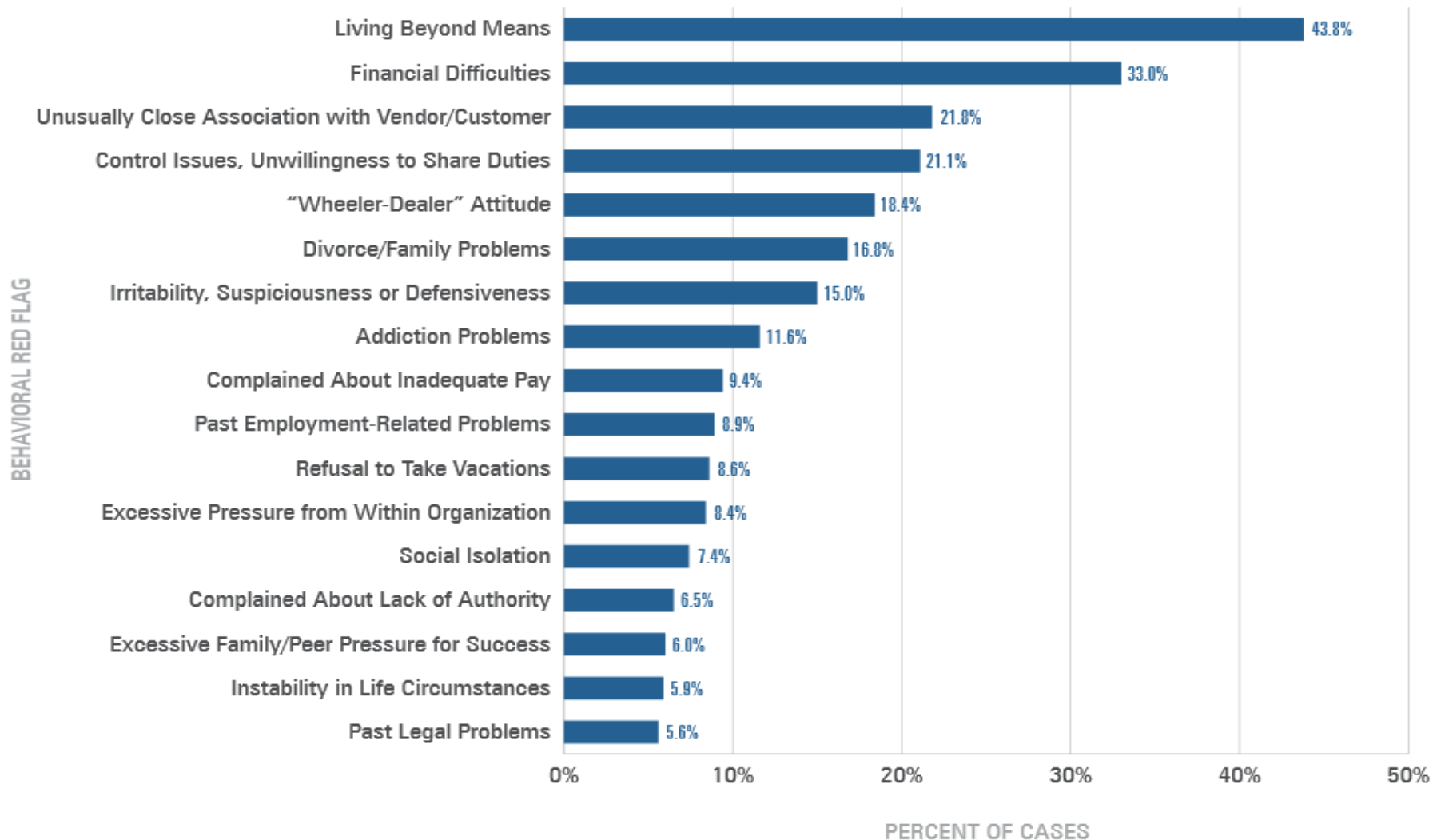
# Median Loss Per Age of Embezzler



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

\* Association of Certified Fraud Examiners (ACFE) 2014

# An Embezzler's Behaviors



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

# REAL LIFE – Local Example #1

**A Melbourne woman is accused of embezzling more than \$650,000 from a medical business to fund a lavish lifestyle, agents announced today.**

by Kevin P. Connolly, Staff Writer



*Christie Hunt*

## ***Points from the article:***

- Ms. Hunt was accused of embezzling more than \$650,000 from a medical business to fund a lavish lifestyle.
- She allegedly diverted funds from her former employer into shell corporations under her name for two years while she was an office manager.
- "Hunt used the money to rent an upscale home, buy furnishings and electronics as well as the purchase of two 2014 Audi Q7 automobiles," the Brevard County Sheriff's Office said in a statement.
- She was being held at the Brevard County Jail on a \$940,000 bond.
- "At the time of Hunt's arrest, members of the Economic Crimes Unit served a search warrant at her residence and seized property and vehicles from the home that are believed to have been the proceeds of her illegal enterprise," the statement added.
- Her duties included financial management, marketing and business development.

# REAL LIFE – Local Example #2

## Accused embezzler said money was owed her for answering emails, etc.

by Austin L. Miller, Staff writer



Kathryn Evelon Swearingen

### ***Points from the article:***

- Ms. Swearingen had been employed at the office for more than 20 years and resigned in mid-August 2012.
- The doctor first found out there was something wrong by receiving notices from the Internal Revenue Service stating he had not paid them enough money for payroll taxes, and he claimed Ms. Swearingen was the person who completed the payroll checks (according to reports).
- From 2009 to 2012 she wrote 243 checks to herself that totaled about \$359,458, and from 2009 to 2011 she only reported about \$132,388 in income compared to about \$278,013 in checks she wrote to herself during that time period.
- She was accused of embezzling more than \$350,000 from the practice and charged with grand theft.
- Ms. Swearingen did not feel she was stealing because the money was "owed to her for each time she was sent or looked at an email; answered texts and phone calls during days, nights, holidays and vacations; and from being on call when they weren't paid for it,".
- She admitted the additional funds were not reported to the IRS.

# REAL LIFE – Example #3

## Chapin accountant pleads guilty to \$1.9 million embezzlement fraud

By HARRISON CAHILL & contributions by Staff writer John Monk



Chandra Padgett

### ***Points from the article:***

- Ms. Padgett pleaded guilty to charges related to the embezzlement of \$1.9 million, and is facing a 25 year maximum sentence with no priors.
- She was the trusted accountant who created a fraudulent shell company called Padgett Specialty Scrapbook Service (PSS).
- Ms. Padgett created checks made payable to her company PSS and hid them among the legitimate invoices by disguising the payments to Physicians Sales & Services (PSS), a legitimate company.
- She falsified adjustments to her salary and had the money deposited directly into her bank account and American Express cards.
- Ms. Padgett owes \$289,032 in back federal taxes for her income of \$849,967 from the year 2011, and constitutes a willful “attempt to evade and defeat the income tax due”.
- Several years ago the doctor noticed “liquidity problems” and hired a forensic accountant who discovered a problem with money being siphoned out of the accounts.

# Key Points for Embezzlement

- The five key areas within a practice that need the most focus:
  - 1) Cash Receipts
  - 2) Cash Disbursements
  - 3) Payroll
  - 4) Computer Access
  - 5) Inventory Controls
  
- Findings from an ACFE study on several cases of fraud:
  - Reviewed the time frame from when the fraud first occurred to when it was discovered.
  - The median found was 18 months!

# Indicators of Embezzlement

- Increase in patient adjustments
- Increase in bad debt write-offs
- Increase in overhead
- Decrease in collections
- Decrease in job performance
- Employee lifestyle changes
- Disorganized books
- Unusual employee behavior
- Large or unusual adjustments on bank reconciliation
- Low collection percentages
- Discrepancies between bank deposits and posting
- Abnormal number of expense reports items
- No cash in deposits
- Large amounts of overtime pay or payroll costs are increasing
- Vendors being paid who you do not recognize
- Increase in patient refunds



# Impact of Embezzlement

## What results from being Embezzled:

- ▶ Financial loss
- ▶ Cost of investigation
- ▶ Reputation
- ▶ Damaged relationships
- ▶ Negative publicity
- ▶ Loss of employees, patients
- ▶ Litigation
- ▶ Damaged morale

# Examples of How it Can Happen

- ❑ Cash payments - reduce the charge amount in the patient's record but charge the accurate amount.
- ❑ Write offs - post the charges, but keep cash.
- ❑ Checks – forge signature, use signature stamp, and/or make copies of new checks.
- ❑ Business Credit Card – Use and manipulate the statement, and/or set up an unauthorized business credit card.
- ❑ Refunds - written to fictitious patients.
- ❑ Vendor/Supplier Payments – pay vendor twice and then use refund.
- ❑ Computer – payments backdated and/or deleted.
- ❑ Vendor Payments – fake company set up by employee, or real payment is going to the employee.

# Examples of How it Can Happen

- ❑ Payroll checks - hours not worked, vacation & sick days, salary increase, and/or “ghost” employee.
- ❑ Adjustments – with payments received and/or expense items.
- ❑ Inventory/Equipment – Selling on Ebay and/or Craig’ s List.
- ❑ Expense reimbursement - Non-legitimate expenses
- ❑ Patient Payments - adjusted or not entered, and checks being cashed.
- ❑ Lapping – involves second set of books utilized in keeping track of manipulation of patient payments.
- ❑ Practice “Dummy” Account – part of checks to deposit going to a second unauthorized checking account.

**Over 1,000 ways this can be done!**

# #1 Type of Fraud in Healthcare

- ▶ Insurance Fraud - accounts for between \$50 to \$100 billion in fraudulent claims.
  - Billing for services not provided
  - Up-coding—Recording a higher level of service than what was actually performed
  - Submitting a claim under one patient's name when services were actually provided to another patient

*This is mix of owner and/or employee involvement,  
so not always involving embezzlement!*

# How was the Embezzlement Discovered?

- The practice owner, alone in the office, happens to receive a phone call.
- The employee was out of the office.
- The CPA discovered it.
- The practice changed CPAs.
- After termination of the employee.
- The doctor was turned down for a business or personal loan.
- There was a practice transition.
- Changed to a new bank and business checking account.
- New practice management software.
- The doctor happens to get the mail.
- New medical biller.

# Goals When Embezzlement is Discovered

- (1) Minimize future losses
- (2) Preserve evidence
- (3) Maximize Recovery

# Referring to Law Enforcement Statistics

<u>Why Not Referred to Law Enforcement</u>	<u>Cases Referred to Law Enforcement</u>		<u>Results of Cases Referred to Law Enforcement</u>	
	<u>Referred</u>	<u>Not Referred</u>		
	60.90%	39.10%		
1 . Fear Bad Public Relations			Pled Guilty / No Contest	56.50%
2 . Disciplined Internally			Convicted at Trial	18.20%
3 . Private Settlement			Declined to Prosecute	15.40%
4 . Too Costly			Other	9.00%
5 . Other			Acquitted	0.90%
6 . Lack of Evidence				
7 . Civil Suit				
8 . Perpetrator Disappeared				

<u>Recovery of Losses</u>	
<u>% Recovered</u>	<u>% of Cases</u>
None	58.40%
51% to 100%*	25.20%
1% to 50%	19.40%
* Note 100% Recovery = 13.6% of Cases	

# Know the DO's and DO NOT's

## **DO!**

- ✓ Act normal & Keep suspicions to yourself
- ✓ Stealth is paramount and that nothing should be done to alert staff that you have concerns
- ✓ Understand the difference between SUSPECTED embezzlement and CONFIRMED embezzlement
- ✓ Make a complete backup of healthcare software data and take it off site
- ✓ Recognize the need for specialized advice
- ✓ Ensure communication with investigators is secure
- ✓ See if your “employee dishonesty” insurance coverage can be increased

## **DO NOT!**

- ✓ Blame yourself
- ✓ Contact police at this point
- ✓ Contact any affected insurance companies yet
- ✓ Ask unusual questions of staff or to ask staff for extra reports
- ✓ Confront the employee
- ✓ Terminate an employee, even if you are “pretty sure”
- ✓ Make any changes to banking arrangements, computer software (such as an upgrade to the latest software version) etc.



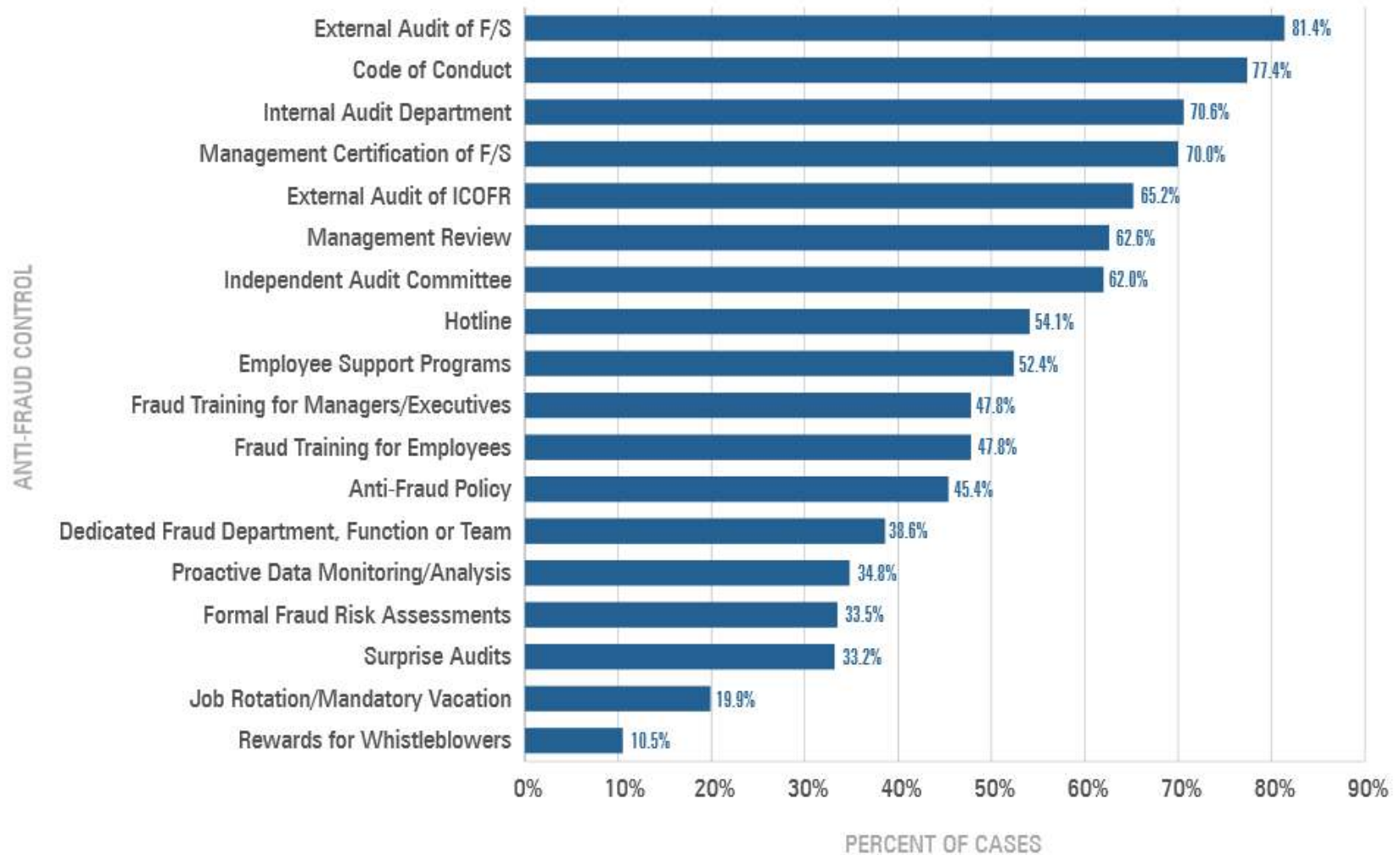
## SECTION #2

**HERE IS YUNG!**

# Establish Safety Measures!

“What Do YOU Do To Protect Your Practice from Embezzlement?”

# Best Practices to Deter Embezzlement



\* Association of Certified Fraud Examiners (ACFE) 2014

# Possible Security Measures

- ✓ Financial Statements –
  - Have them mailed to the physician's home, PO Box, and/or CPA
  - Utilize statements online instead of paper
- ✓ Patient Credit Cards –
  - Have a security code installed on your merchant terminal for refunds
  - DO NOT write down a patient's credit card information anywhere!
  - Keep a patient's credit card information securely and electronically stored where it is off site and employees can only view the last digits of the card number!
- ✓ Engage your CPA/Consultant to do periodic "audits".
  - The key here is random
- ✓ Compare the receipts per the day sheet to the bank deposit receipt.
  - If you do not have a Day Sheet....get one!

# Additional Possible Security Measures

- ✓ Hiring Practices for Staff -
  - Carefully check references!
  - Perform background checks (Pay for the service!)
  - Bond employees from day 1
- ✓ Direct all checks coming via the mail to a bank lockbox
- ✓ Insist that all transactions be documented
- ✓ Get rid of Signature Stamps!
- ✓ Employees
  - Segregate duties
  - Cross-train employees
  - Everyone takes a vacation
  - No one at the practice alone
  - Time Clock = All punch in and out
- ✓ Make sure checks are stamped immediately with “For Deposit Only”

# And More Possible Security Measures

- ✓ Periodically review accounting entries rather than just checking totals
- ✓ Compare the schedule and sign-in sheet to the day sheet every day.
  - “No show’s” versus who really did show!
- ✓ At the end of the month, compare total deposits on the bank statement to total receipts posted in the computer.
- ✓ Compare charges, receipts and adjustments to prior periods and years.
- ✓ Calculate collection percentages and compare to prior periods.
- ✓ Inventory Controls -
  - Keep a log for stock in / out, and audit monthly.
  - Put a security camera in the room.
  - Review monthly associated expense to see if “reasonable”
- ✓ Healthcare IT Security -
  - Hire to keep computers secure from outside and inside!
- ✓ Cash Controls -
  - Locked at all times and dual control for opening and closing.

# External Fraud – Where are the Risks?

60% of organizations were exposed to actual or attempted payment fraud in 2013\*

- ▶ 27% of financial professionals that experienced payments fraud in 2013 report the number of fraud incidents increased from 2012.
- ▶ 82% of survey respondents report that checks were the primary target for fraud attacks at their companies.
- ▶ 43% of survey respondents from organizations exposed to fraud attacks report credit/debit cards were targeted.
- ▶ The typical financial loss incurred by companies due to payments fraud in 2013 was \$23,100.
- ▶ 16% of financial professionals from organizations that experienced payments fraud report a decrease in fraud incidents in 2013 compared to 2012.

“The vulnerability of all payment methods to fraud demands a range of fraud-fighting tools and the vigilance of those responsible for protecting the assets of their organizations” \*\*

\* Based on the 2014 AFP Payments Fraud and Control Survey

\*\* Based on the 2013 AFP Payments Fraud and Control Survey

# Timeframe to File a Fraud Claim

- ▶ ACH Debits
  - 48 Hours Business 2 Business
  - 60 Days Consumer 2 Business
  - \* Exceptions – Banks are typically liable to return consumer debit items for up to 24 months if they cannot demonstrate appropriate authorization.
- ▶ Positive Pay
  - Forged maker signature/Counterfeit - the law states 30 days from date of statement, but some banks will allow up to 60 days and often pays the claim if they are brought to them within that time frame.
  - Forged Endorsement Claims - 3 years
- ▶ Business Options
  - 60 Days Business 2 Business
  - 60 Days Consumer 2 Business



# External & Internal Fraud – What Services Help?

Explore with your Financial Institution  
Traditional and Non-Traditional Fraud Tools!

## TRADITIONAL FRAUD TOOLS

- ▶ Positive Pay- various forms
- ▶ ACH Positive Pay
- ▶ UPIC- Universal Payment Identification Code

## NON-TRADITIONAL FRAUD TOOLS

- ▶ ACH Services
- ▶ Lockbox Services
- ▶ Information Reporting
- ▶ Payables
- ▶ Remote Deposit

# Who Can Help?! – Outside Services

## Talk to your Banker!

- ✓ Treasury Management Services that could help deter and/or discover embezzlers.
- ✓ Review your revenue cycle and operations for services that “fit” best.
- ✓ Revenue cycle and operations reviewed quarterly or semi-annually in case there are changes.

## Talk to your CPA!

- ✓ Services offered that could help deter embezzlers.
- ✓ Help with setting up and interpreting bench marking reports and day sheets.
- ✓ Review and implement audit controls.

## Talk to your Insurance Agent!

- ✓ Understand different insurance coverage options:
  - Employee Dishonesty
  - Crime Coverage
  - Fidelity Bond

## Talk to a Practice Consultant!

- ✓ Procedures put in place that can help to deter embezzlers.
- ✓ Review billing and coding.
- ✓ Review collection and payment procedures.
- ✓ Review your payroll process.
- ✓ Get a data security check up.
- ✓ Implement inventory controls.

# EXAMPLE - Embezzlement Risk Assessment



[www.dentalembzezzlement.com](http://www.dentalembzezzlement.com)  
 Priority Help: [emergency@dentalembzezzlement.com](mailto:emergency@dentalembzezzlement.com)  
 Toll free: 888-398-2327

## Embezzlement Risk Assessment Questionnaire

While the methodologies used to steal from a dentist will vary from practice to practice one thing that remains strikingly constant in all embezzlement environments is *observable employee behavior*. Stealing employees behave in a very predictable manner, regardless of the embezzlement method they are employing.

According to a 2007 ADA survey, over two thirds of embezzlements were discovered by observing employee behavior; less than one third was revealed by non-behavioral (i.e. financial) indicia.<sup>(1)</sup>

The following is a checklist of behaviors and other indicators that are consistent with employee dishonesty. Please complete for each "employee group" below that applies to your practice, and total the points for each group. When completing for former employees, questions should be answered as if you were completing this before these employees left your office.

Our recommendation is to re-do this questionnaire every six months. Also, because we are continually improving this form based on our continuing experience with embezzlement, we recommend checking back with us annually to ensure that you have the most up-to-date questionnaire. You can request an up-to-date copy by emailing [fraudnews@prosperident.com](mailto:fraudnews@prosperident.com)

### Questions for the dentist

Question	Former "suspect" employees	Office Manager	All other front desk staff	All non-front desk staff	Score for "yes" answer
1. Do any of your employees face severe financial issues?	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	5 points
2. Does any employee appear to be living beyond their means?	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	5 points
3. Are you aware of any employee with substance abuse issues, a gambling addiction or	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	

# Disclosure

The seminars and/or webinars and materials that you will view were prepared for general information purposes and are not intended as legal, tax or accounting advice or as recommendations to engage in any specific transaction, including with respect to any securities of PNC, and do not purport to be comprehensive. Under no circumstances should any information contained in the presentation, the webinar, or the materials presented be used or considered as an offer or commitment, or a solicitation of an offer or commitment, to participate in any particular transaction or strategy. Any reliance upon any such information is solely and exclusively at your own risk. Please consult your own counsel, accountant or other advisor regarding your specific situation. Neither PNC Bank nor any other subsidiary of The PNC Financial Services Group, Inc. will be responsible for any consequences of reliance upon any opinion or statement contained here, or any omission. The opinions expressed in these materials or videos are not necessarily the opinions of PNC Bank or any of its affiliates, directors, officers or employees.

PNC is a registered mark of The PNC Financial Services Group, Inc. (“PNC”)

©2015 The PNC Financial Services Group, Inc. All rights reserved.

# Speaker Contact Information



- Jeff Holt, Healthcare Business Banker

[Jeffrey.Holt@PNC.com](mailto:Jeffrey.Holt@PNC.com) / Ph#: (352) 385-3800

- Yung Nguyen, Healthcare Treasury Management Officer

[Yung.Nguyen@PNC.com](mailto:Yung.Nguyen@PNC.com) / Ph#: (813) 221-6145

Website: [www.pnc.com/hcprofessionals](http://www.pnc.com/hcprofessionals)

**\* REFERRALS ARE GREATLY APPRECIATED! \***