Pilfering For Pleasure:  
Is Your Practice Vulnerable to Embezzlement? 

*White Paper*

**MARCIA WHITE, MPA**
Manager

July 2016

**CONTACT**
For further information about Coker Group and how we could be of assistance, call 800-345-5829 x137 or visit www.cokergroup.com.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Fraud Versus Embezzlement</td>
<td>3</td>
</tr>
<tr>
<td>Risk of Embezzlement</td>
<td>4</td>
</tr>
<tr>
<td>Risk Across the Nation</td>
<td>4</td>
</tr>
<tr>
<td>Risk in the Practice</td>
<td>5</td>
</tr>
<tr>
<td>Rule of Thumb and the Motivations</td>
<td>5</td>
</tr>
<tr>
<td>Understanding The Fraud Triangle</td>
<td>6</td>
</tr>
<tr>
<td>Minimizing Opportunity and Instituting Checks and Balances</td>
<td>7</td>
</tr>
<tr>
<td>Three-step Risk Management and Mitigation Process</td>
<td>7</td>
</tr>
<tr>
<td>Establish Basic Protections</td>
<td>9</td>
</tr>
<tr>
<td>The Anatomy of Embezzlement</td>
<td>9</td>
</tr>
<tr>
<td>What’s Next?</td>
<td>14</td>
</tr>
<tr>
<td>Suspecting Embezzlement</td>
<td>14</td>
</tr>
<tr>
<td>Terminating and Prosecuting</td>
<td>15</td>
</tr>
<tr>
<td>Taking Action</td>
<td>15</td>
</tr>
<tr>
<td>Summary</td>
<td>15</td>
</tr>
<tr>
<td>Resources</td>
<td>16</td>
</tr>
</tbody>
</table>
Abstract: Articles abound about the prevalence of theft in the business world, yet few writers give sufficient examples and safeguards against losses for implementation in the medical practice realm. The losses due to theft are startling and more damaging than many practice owners may realize. With the pressures of the evolving healthcare system, physicians have little time to monitor many of the business aspects of their practices and naturally prefer to entrust their finances to their few employees. This article, using credible statistics, establishes the astounding losses and exposes the vulnerabilities that are typical of many smaller medical practices. Case studies present examples of how theft occurs and how to discover it, whether as minimal pilfering or as major embezzlement schemes. Finally, this white paper provides reasonable safeguards to minimize the opportunity for financial losses to occur.

Key Words: embezzlement, pilfering, theft, fraud, opportunity, financial pressure, rationalization, safeguards, mitigation, zero tolerance, prosecution

INTRODUCTION

With widespread changes to the health care system occurring, physicians now have to focus on population health management, accountable care organizations, alignment, new electronic health records and technology, and other urgent demands for their attention. The distractions of the immediate often cause the physician to overlook the business aspects of their practice. However, rather than ignore the day-to-day operations, there is an increasing need to expand efforts and efficiencies on the revenue cycle and analytics, especially in matters of the loss of revenue due to embezzlement. A rise of incidences of pilfering is occurring across the country, and physician practices are vulnerable targets.

The purpose of this paper is to introduce the magnitude of in-office theft and the gravity of the effect on medical practices. The reader will learn the importance of establishing structure and safeguards for reducing the opportunity for embezzlement. Case studies will be used to explain how vulnerabilities arise and how to uncover them. The goal is to reinforce financial safety in your practice for your optimum success.

FRAUD VERSUS EMBEZZLEMENT

Physicians, healthcare providers, insurance companies, and even the Centers for Medicare and Medicaid (CMS) have an expanding awareness regarding fraud. In fact, CMS has taken great strides to counteract the abuses from fraud through the implementation of and enforcement of federal regulations like the False Claims Act, Anti-Kickback Statute, and the Stark Law.
Healthcare fraud is characterized by:

- Knowingly submitting false statements or making misrepresentations of fact to obtain a healthcare payment for which no entitlement would otherwise exist;
- Knowingly soliciting, paying, and/or accepting remuneration to induce or reward referrals for items or services reimbursed by healthcare programs; or
- Making prohibited referrals for certain designated health services.

Although fraud has been a focus of attention in medical practices, what is less noted is the financial loss within the practice due to theft by embezzlement. While many people often use the term as the descriptor of fraud, the definition of embezzlement is “the fraudulent conversion of another’s property by a person who is in a position of trust, such as an agent or employee.”

Embezzlement, simply stated, is knowingly or intentionally taking someone else’s property (or money) by an employee or person who is entrusted to handle the money.

Statistics from The 2013 Marquet Report on Embezzlement show an increase in embezzlement across the country, and the losses are significant. Although this report is from 2013 and reported in 2014, many of the statistics are used as a benchmark in 2016.

- The Global Median loss across all industries = $150,000
- 71% incidents were committed by employees who held financial, bookkeeping, or accounting positions
- The most common embezzlement scheme involved forging and tampering with checks
- The average scheme lasted 4.6 years
- 94.5% of the time the perpetrator takes effort to conceal the fraud
- Nationally, nearly three-fifths (57%) of the incidents were committed by women. This percentage increases significantly in the healthcare industry where the percentage of women perpetrators was 82%
- The median age of the perpetrator was 50 years old

**RISK OF EMBEZZLEMENT**

**RISK ACROSS THE NATION**

According to The 2013 Marquet Report on Embezzlement, 2013 was a banner year for embezzlement and outpaced the previous 5-year period. In 2013, 554 major embezzlement cases were active in the U.S., which represents more than 10.5 cases per week and indicates a 5% increase over the previous year’s cases. Financial stress due to economic downturn is a factor in potential embezzlement cases. In recent years, the desire to live a more lavish lifestyle appears to be the motivation for embezzlement rather than financial misfortunes as denoted in previous years.
Healthcare embezzlement cases accounted for 5.7% of the total cases in 2013, accounting for $44,975,000 (or 7.6% of the total national loss) with an average loss in healthcare of $1,450,806. By total loss, healthcare was second to the financial services industry.

**RISK IN THE PRACTICE**

The Association of Certified Fraud Examiners (ACFR) estimates that the typical organization loses 5% of its revenues each year to embezzlement, which equates to approximately $27 million in total losses annually.\(^\text{10}\)

Embezzlement will strike an estimated three out of four medical practices in the United States. Small practices with less than 100 employees are more vulnerable than larger practices. This factor is partly due to the overall perceived loyalties and trust with the employees in the practice. On average, employees with 10 or more years of service commit 25.2% of embezzlement crimes.\(^\text{11}\) Further, small practices are more vulnerable due to the inability to have the necessary checks and balances in place. While larger practices tend to have policies and procedures and oversight with the management of critical financial functions, smaller practices do not have the time or resources to set up these policies and procedures. Figure 1 shows the potential median total annual revenue for an individual provider and indicates the revenue loss at 5%.

**Figure 1**

*The Potential Financial Impact to a Single FTE Physician\(^{12}\)*

<table>
<thead>
<tr>
<th>Specialty</th>
<th>Median Total Revenue/FTE Physician</th>
<th>5% Loss to Embezzlement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardiology</td>
<td>$618,883</td>
<td>$30,945</td>
</tr>
<tr>
<td>Orthopedic Surgery</td>
<td>$804,335</td>
<td>$40,217</td>
</tr>
<tr>
<td>Family Medicine</td>
<td>$471,190</td>
<td>$23,560</td>
</tr>
<tr>
<td>ENT</td>
<td>$688,076</td>
<td>$34,404</td>
</tr>
<tr>
<td>OB/GYN</td>
<td>$605,041</td>
<td>$30,252</td>
</tr>
</tbody>
</table>

**RULE OF THUMB AND THE MOTIVATIONS**

It is not uncommon for individuals to dream up elaborate schemes to commit fraud and embezzlement from medical practices. The generally accepted rule of thumb (see Figure 2) is that 10% of employees will always steal (given any opportunity); 10% of employees will never steal (no matter what); and 80% of employees will steal when under the right set of circumstances (depending on how they might rationalize the particular opportunity). Therefore, it is important to focus on the 80% and direct energy toward prevention and reduction of risk to the practice on that subset of employees.

**Figure 2**
Many factors motivate employees to steal, and there are a wide variety of personality traits that drive this behavior.

**Motivation for Stealing**

- Living beyond one’s means
- Desire for personal gain
- Feeling challenged to “beat the system”
- Excessive habits
- Extreme pressures
- Close association with patients

**Personality Traits**

- Extremely well liked by staff and patients
- “One of the family” — the employee routinely invited the entire office to family events such as weddings
- Very proficient at their job and hard-working, often to the point of working extra hours and taking work home
- Rarely take vacations or days off
- Given responsibility for numerous functions related to handling practice finances, including patient payments and accounts, bank deposits, and balancing/reconciling the practice’s checking account
- Takes total control of their area of job responsibility, is protective/possessive of their “turf”, and becomes “the general” in the office
- Extremely defensive when questioned about irregularities and always has a plausible excuse for missing funds or imbalances

**Understanding The Fraud Triangle**

There are three factors, that when combined, lead to why honest people steal from their employers. (1) Financial pressures (e.g., medical bills, mortgage payments, or extensive debt); (2) rationalization for stealing from you (i.e., they are doctors, they can afford it; or “I am just going to borrow it”), and (3) opportunity (i.e., how easy it is for them to steal and they won’t get caught). Figure 3 illustrates this theory, which is known as the Fraud Triangle.

The only element an employer has control over is minimizing opportunity; specifically, this occurs by reducing the risk of the three elements that create opportunity in a practice.

1. Complete trust in individuals
2. Concentrations of responsibilities and duties performed by one person
3. Little or no oversight to important aspects of everyone’s job
MINIMIZING OPPORTUNITY AND INSTITUTING CHECKS AND BALANCES

Various types of schemes exist when it comes to employees embezzling from a practice. Stealing cash before or after recording it on the practice’s books is the primary pattern employees use to take from the practice. Also, pilfering petty cash, forging checks, or submitting invoices for fictitious goods or services collectively comprise 75% of the ways employees embezzle. Figure 4 charts the various schemes of embezzlement.

Figure 4

THREE-STEP RISK MANAGEMENT AND MITIGATION PROCESS

The three steps in risk management and mitigation process encompass assessment of high-risk areas, complete segregation of duties, and monitoring and auditing of the vulnerable areas.

Assessment of High-Risk Areas: The first step in risk management and the mitigation process is to assess and audit the high-risk areas within the practice. The performance of an annual evaluation of policies, procedures, and processes should occur for areas deemed “high-risk”, including front-office cash collections, processes as they relate to data entry of cash into the practice management system, and any areas where new software or people have changed in the past year. This evaluation will allow the practice to identify gaps where checks and balances need to be in place.

Complete Segregation of Duties: The second step is to create a significant separation of functions. This segregation of duties is critical when employees have responsibilities that relate to the overall revenue cycle process. For example, the front office reception personnel who take in copays should not have full access to the practice management system and should not have the authority to “write-off” balances within the software system.
Often, all employees are given all “rights” or “permissions” to the software system, allowing them to have the ability to change any part of the patient’s overall balance. Rather, the goal should be that the same person who authorizes transactions cannot record them and will not have access to the assets (i.e., bank account, money). This separation of “rights” is difficult for a small practice and sometimes the division of duties seems impossible.

**Monitoring and Auditing:** The third critical step of risk management and the ability to mitigate risk is through surveillance and auditing. This step is crucial as it sets the “tone” of the practice from the top down. Figure 6 shows the main components related to monitoring and auditing to protect your practice against embezzlement.

![Figure 6](image)

Establishing a zero tolerance policy and creating a code of conduct upon hiring of employees defines and sets expectations from the beginning. It is important to create an environment for the protection of those who want to discuss suspicious behavior, as 39.1% of cases detected are through “tips.” Many organizations have established a whistleblowers’ hotline service for employees to report suspicious behavior. Statistics show that organizations that used hotlines were more likely to detect fraud (47%) versus those organizations without hotlines (28%).

Monitoring the practices finances through routine and surprise audits and reconciliations helps mitigate the opportunity for embezzlement and catches any ongoing embezzlement that may have already begun. These precautions ensure that all checks, purchase orders and inventory, and invoices and payments align and accurately reflect the financial activity of the practice.

When hiring new employees, background and credit checks can be helpful to weed out any potential employees with a history of embezzlement. This research provides the information needed to make the best staffing decisions up front and potentially avoid later issues. (Background checks can be unreliable in the discovery of embezzlement, however, as many healthcare employers are hesitant to bring charges of theft against employees.)
ES TABL I SH BASIC PROTECTIONS

It is important in any practice to create some basic protections. As previously mentioned, opportunity is the only aspect of the three-pronged triangle that the practice can control. In addition to the three-step risk management and mitigation process, establishing basic protections is critical to minimizing the opportunity and mitigating the risk of loss through embezzlement. Figure 7 provides a checklist to use as a reference.

**Figure 7**
The Do’s and Don’ts to Protect Your Practice

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Do avoid having only one person handle the finances.</td>
<td>- Don’t ever sign blank checks.</td>
</tr>
<tr>
<td>- Do run surprise audits.</td>
<td>- Don’t have only one person sign checks.</td>
</tr>
<tr>
<td>- Do stamp “For Deposit Only” on all checks.</td>
<td>- Don’t use signature stamps.</td>
</tr>
<tr>
<td>- Do use a lock box; deposit electronically.</td>
<td>- Don’t overlook signs of disgruntled employees.</td>
</tr>
<tr>
<td>- Do follow up on patient complaints regarding overpayments.</td>
<td>- Don’t have obvious passwords.</td>
</tr>
<tr>
<td>- Do create an incident reporting system for employees to report</td>
<td>- Don’t hire employees without performing a background and credit</td>
</tr>
<tr>
<td>suspicious behavior.</td>
<td>checks.</td>
</tr>
<tr>
<td>- Do review accounts payable vendors to avoid fictitious vendors.</td>
<td>- Don’t have the same person work accounts payable and reconcile the</td>
</tr>
<tr>
<td>- Do get an insurance policy that covers employee theft.</td>
<td>bank account.</td>
</tr>
<tr>
<td>- Do watch for those who express financial difficulties or have a rise</td>
<td>- Don’t borrow money from petty cash or cash receipts.</td>
</tr>
<tr>
<td>in living standards.</td>
<td>- Don’t give out credit card numbers to employees.</td>
</tr>
<tr>
<td>- Do be weary of those who won’t take a vacation.</td>
<td></td>
</tr>
<tr>
<td>- Do change passwords often.</td>
<td></td>
</tr>
</tbody>
</table>

THE ANATOMY OF EMBEZZLEMENT

The following case studies are examples of how embezzlement can occur in a medical practice. Each study presents how the scheme was discovered, what to look for, and how to avoid the incident.

**Case #1 – Happy Holidays:** A small, three-physician psychiatry practice allowed all employees unlimited access to the practice management software system, including the front-office reception employees. In this case, the front-office staff had access to collect cash copayments from the patients. The employees had access both to post the amount and to write-off the amount as a contractual adjustment in the system. Since the amount was written off to an adjustment, there was no record of accepting the money. Further, no additional billings were
sent to the patient, as it appeared the patient had no balance. Figure 8 illustrates the process of the scheme used in the case.

**Figure 8**

![Diagram](image)

**Diagnosis of Case #1**

**How was this caught?**

One of the front desk personnel left for maternity leave, and a physician’s wife filled in for the person on leave of absence. The physician’s wife realized more money was being deposited into the bank account than in previous months and questioned the discrepancy.

**What to look for in discovery?**

This situation began with a suspicion and a simple math equation. For example, the number of visits/day multiplied by the average dollars of a copay multiplied by the average days in a month should be similar from month to month. The equation should have consistently been 10 visits/physician multiplied by $20 multiplied by 20 days/month = $4,000 deposited in bank/physician/month. This result was not the case in previous months, when the average monthly deposit was $400 in bank/physician/month.

**How could this crime be avoided?**

- Allow front desk personnel access to receive the transaction and print a patient receipt for the visit but not full access to record the amount and write-off the payment in the practice management system.
- At a minimum, use and post a numbered receipt book in the practice management system, and/or issue the patient a numbered receipt from practice management system.
- A second person should review receipts and run the daily deposit report at the end of the business day. This report should match the practice management system’s report.
- A second person should fill out the bank deposit and, if necessary, should make the deposit.

**Case #2 – Family Fun:** A 10-physician orthopedic practice allowed all employees the same software access for front-end and back-end operations within the practice management system. In fact, all staff rotated between the front-end and the back-end operations. All employees were allowed to have access to appointment scheduling, patient collections, and insurance collections. This case is similar to Case #1 but was a more elaborate scheme and involved a supervisor and family members. In this case, the orthopedic practice allowed patients without insurance an automatic discount for services rendered, but the amount would be determined by the supervisor (between 20% and 50%), depending on the service provided. When the patient (a friend or family member) would come in for the service, the supervisor would enter the patient payment at a 20% discount (this was not actually paid by the patient). When the discount was entered in the system, it was recorded as a 50% discount, producing an overpayment in the system. The recorded overpayment was refunded to the patient and split between the family member and the supervisor. Figure 9 tracks the steps in the pilfering scheme.

**Figure 9**

Self-Pay Patient Services Rendered → Balance Due From Patient = $1000 → Practice Allows Up to 50% Discount → Supervisor Gives Patient 20% Discount

Patient Payment Entered (Not Paid) = $800 → Supervisor Records Cash Discount of 50% Instead of 20% ($500 vs. $800) → Supervisor Records Overpayment on Friend or Family Account → Daily Deposit Balances

Refund Check Made Out to Family or Friend of Supervisor for $300 → Money from Overpayment Split Between Family or Friend of Supervisor

**Diagnosis of Case #2**

**How was this caught?**

The external bookkeeper noticed multiple payments to the same person and wondered what was wrong with this person because they were seeing the physician so regularly. When questioned, the supervisor had numerous excuses. Eventually, the bookkeeper asked the physician about the transactions, and they determined
that the patient had seen many of the physicians in the practice multiple times for the same procedure.

What to look for in discovery?

A significant amount of refunds and overpayments made to patients, and lack of security and access regarding practice management software.

How could this be avoided?

- Define an amount of self-pay discount (set at a certain number)
- Conduct a thorough investigation of refunds (both insurance and patient)
- Segregate duties of collecting cash and posting of payments
- Institute a financial policy to be signed by the patient, and provide a copy of the receipt to the patient for the agreement

Case #3 – The Phantom Vendor: A 20-year seasoned optical technician in an 18-provider ophthalmology practice was responsible for ordering and receiving all the supplies for the retail optical shop as well as the supplies for the ophthalmology practice. The practice regularly ordered from several vendors. This case is a very classic one where a phantom vendor enters the mix, which included phantom purchase orders and phantom supplies. The ordering technician created the phantom vendor and set up bank accounts to receive all payments to the phantom vendor. Figure 10 walks through the steps of this scheme’s process.

![Figure 10](image)

Diagnosis of Case #3

How was this caught?

A physician was looking for the “phantom product” after seeing it on an inventory list and could not find it. The physician began to question the ordering technician,
and eventually, suspicion was raised regarding the amount ordered over time and the non-existent product.

**What to look for in discovery?**
Review invoices and verify that the supplies are relevant to the practice.

**How could this be avoided?**
- Segregate the duties between order person and intake person
- Establish that a provider has the final say in approving vendors
- Review vendors periodically and send out RFPs for bids

**Case #4 – Credit Card Trickery:** An 8-provider OB/Gynecology clinic with a single waiting area and a four-lane patient check-in station used credit card readers to accept copays and balances due from patients. Each lane had an individual card reader. One receptionist, a long-time employee who had seen the practice grow from two physicians to multiple providers, still had access to all the practice information.

In this case, the employee had dealt with many of the sales vendors over the years, and a new merchant vendor wanted the practice to try their new merchant machine. The receptionist agreed (and had the authority) to test the merchant’s device at one of the check-in stations. The receptionist had set up a bank account with a similar name to the practice in her name and had given the new merchant sales representative the information for the account. When incoming patients used the station with the new merchant machine, the money was deposited directly into the receptionist’s account.

The new merchant account was only to be for a short trial period; however, the practice was too busy to stop the account. Therefore, the trial period lasted over a year. Follow the steps in Figure 11 to see the progression.

![Figure 11](image-url)
Diagnosis of Case #4

How was this caught?
The physicians of the practiced decided to “earmark” the money that came in through copays to use for employee bonuses. As they began checking from previous years, they realized that the account balance was less than in prior year.

What to look for in discovery?
- Reduction in copays
- Employees that have access to documents, statements, or records that aren’t their usual line of work

How could this be avoided?
- Personal/Practice information should never be accessible except for specific personnel
- Decisions about new equipment, etc., should be made with the provider
- Audit any new process when adding new equipment or making software changes
- Produce daily deposit reports and checks and balances with the bank account

What’s Next?

Suspecting Embezzlement

What do you do if you suspect embezzlement in your practice? First, begin by gathering relevant documentation and accounting records, and make notes regarding observations and behaviors (recording dates and times). At this step, it is important to collect information and documentation, which could eventually develop into legal evidence. The collection of this information will force a decision on whether or not there is an issue regarding embezzlement. This discovery process unearths an understanding of the potential amount and duration of the theft.

Second, if a determination of possible wrongdoing occurs, it is essential to contact an attorney, the practice accountant, and the police to notify them of the possible of the fraudulent act. Further, all potentially dishonest employees (it could be more than one, and it could even be a provider or partner) must be removed from the workplace immediately. Also, note that when an owner or executive commits theft, the median damage is far more significant than when an employee steals. Statistics show that the loss is more than ten times greater than when employees were the perpetrators.19

Although not all insurances cover employee theft, it is essential to contact the practice’s insurance company to report the potential loss. Often, the insurance company will have specific requirements and documentation that is necessary for the practice to file a claim. Further, some
insurance companies have internal personnel who can help guide the practice through the claim process.

**TERMINATING AND PROSECUTING**

Once it is determined that the employee has embezzled from the practice, a decision of the best course of action is needed. Should the practice terminate the employee and prosecute the charges? Estimates are that seventy (70%) of those who commit acts of embezzlement in a healthcare practice have pilfered previously at other medical practices (which is significantly higher than in other industries where most fraudsters are first-time offenders). About 29% of embezzlers at practices are prosecuted, and about 82% are terminated from their jobs. Thus, those who are not prosecuted can move from practice to practice.

**TAKING ACTION**

There is no “fool-proof” way to ensure a medical practice will not fall prey to an employee who decides to embezzle. Financial pressures and rationalization will always be prevalent, and the only defense is to minimize the opportunity to steal through safeguards. Establishing the three-step risk management and mitigation process (see figure 5) will create a foundation for prevention and mitigate the risk of loss.

Successful practices acknowledge and strive to create a trusted yet accountable office culture. There is a balance between having too much trust in employees and being overly-suspicious. Establishing the zero tolerance practice culture from the beginning is important as well as having all employees (and physicians) follow the same policies and procedure throughout the organization. There are some basic do’s and don’ts that a practice should support that are not difficult to implement.

Lastly, many embezzlers in healthcare tend to be fired from one practice and then hired at another because few ever undergo prosecution. Thus, do not hesitate to bring an action against the embezzler that calls for establishing a repayment plan or even jail time for the perpetrator.

**SUMMARY**

The wide-spread problem of embezzlement in healthcare, whether incidents of pilfering or grand theft, is massive and more damaging than many practice owners may realize. The statistics of losses are startling—and increasing. Even “honest people”, when exposed to financial pressures and other factors, are apt to steal when the temptation is too great. Although no organization is completely theft-proof, many safeguards, beginning with a no-tolerance for theft policy, can be set in place to minimize the opportunity for embezzlement.
RESOURCES

17. Ibid.
18. Ibid.
19. Ibid.