THEFT

in group practices costs billions of dollars annually

Warning: New MGMA research shows that "honest" employees embezzle

By Denise McClure, CPA, CFE, president of Averti Fraud Solutions LLC, denise@avertifraudsolutions.com, with data analysis by James Margolis, MPA, FACMPE, MGMA, jwm@mgma.com

Given the choice to increase revenues by 5 percent or lose millions – or billions – to fraud, what would you do?

It is a choice, yet few professionals recognize it. As a result, medical practices lose $25 billion annually, according to the Association of Certified Fraud Examiners (ACFE). The group estimates that the typical organization loses 5 percent[1] of its revenues to fraud each year. Apply that number to the 2008 national physician and clinical services expenditures[2], and it becomes $25 billion.

In the 2010 ACFE report, 86 percent of perpetrators were first-time offenders[3] who had never been charged or convicted of a fraud-related offense.

MGMA members are not immune, according to Association research of 946 respondents conducted in November and December 2009.

MGMA members reported 782 cases of theft totaling $94,603,779 in losses. In these cases, employees stole through theft of receipts, cash on hand, disbursements such as forging or altering a check, submitting fictitious invoices, paying personal expenses with company funds, payroll and expense reimbursement. (See table on page 41.)

Although employee theft of $100,000 or more represented 18 percent of the cases, those high-dollar thefts accounted for 93 percent of the total losses. (See table on page 42.)

In one case, an accounts payable clerk stole $240,000 from a small group (fewer than 10 physicians) in a little over a year. He altered checks to legitimate vendors to make them payable to him. It was discovered by accident, as is often the case with embezzlement, while someone was looking for supporting documentation for a fixed-asset purchase.

How they do it

Employees who stole money worked alone in the vast majority of cases. In more than half the cases, employees had three or more years of tenure.

Most fraud schemes go undetected for long periods. In the MGMA research, it was a median of eight months compared to 18 months for the ACFE survey; however, thefts greater than $100,000 were ongoing for a median of 36 months[4] before being discovered.

Eighteen respondents reported losses of $1 million or more. The million-dollar schemes involved groups ranging from one to several thousand physicians.

One of the cases involved the administrator of a group of fewer than five physicians. For 20 years the person had control of all accounting functions with the exception of month-end financial reports prepared by an outside public accounting firm. The practice lost $1 million over five years through various payroll and cash disbursement schemes. It came to light when the administrator's husband was hospitalized and an outside person was brought in and quickly uncovered the scheme.

Many fraud schemes require constant attention to hide the losses. Any one of the following three internal controls may have prevented or diminished the theft described above:

1. Requiring the employee to take vacations while someone else covers his or her primary responsibilities;

see **Theft**, page 40

Read this article, earn ACMPE credit
mgma.com/ACMPEcredit

MGMA's key research results

- Median loss: $5,000
- Median duration: eight months; 17 percent of thefts went undetected for more than two years
- High-dollar thefts of $100,000 or more accounted for 93 percent of the total losses reported, went undetected for three years and 81 percent involved only one perpetrator
- Two of three thefts of $50,000 or more involved medical groups of 10 or fewer physicians
- Top management perpetrated the theft in over half the cases where the loss was $50,000 or more
- Groups of 10 or fewer physicians accounted for 70% of the cases reported and 63% of the amount stolen; more than half the cases involved groups of five or fewer physicians

2. Reviewing canceled checks, particularly payroll and disbursement checks payable to the employee or to unfamiliar vendors; and
3. Surprise reviews of payroll and cash disbursements by a certified public accountant or forensic accountant.

Of the 116 cases involving thefts of $100,000 or more, 70 percent occurred in smaller groups of 10 or fewer physicians. Perpetrators were typically long-term employees with access to money and the ability to override controls.

A respondent who reported a $150,000 theft described the thief this way: "This employee was in a position of trust and had access to all areas, and violated all areas. You might term her 'morally flexible.'"

The respondent, a forensic accountant who helps protect the practice, offers this advice: "Even in a small office, separation of duties can be achieved. Providers who are reluctant to be the bad guy need to hire and pay someone outside the organization to periodically step in to do a lookover. [This physician] has had no problems since, and all staff [members] are aware that I come with the job before they accept positions. I am not friends with the staff, but I am friendly and able to get the job done with dignity and speed. So far it works for everyone."

Why are medical groups at risk?

All businesses are at risk of employee theft and embezzlement. Medical practices are especially vulnerable because:

- Physicians/owners trust employees to do their jobs with little oversight or interference, creating an opportunity for trusted employees to steal with little risk of being caught. It's important to trust your employees, but checks and balances are a necessity.
- In smaller groups, it is difficult to separate duties because too few people are involved in the accounting processes.
- Medical practices have a high transaction volume, which makes losses less noticeable.

How and why honest people steal

A widely accepted rule of thumb among forensic accountants, auditors and those who write employee dishonesty coverage insurance is called the 10-10-80 rule: 10 percent of your employees will always steal, 10 percent will never steal and the other 80 percent will steal under the right set of circumstances.

In the 1940s a researcher named Donald R. Cressy interviewed about 200 people imprisoned for embezzlement. He excluded those who took a job with the intention of stealing and focused on "trust violators," whom he defined as honest people who crossed the line.

Cressy developed the concept of the "fraud triangle" to describe the following three elements required for someone to commit fraud:

- **Financial pressure** – Regardless of the situation, the perpetrator believes he or she cannot talk about it. It could be an addiction (gambling, drugs, shopping); loss of household income; medical bills; debt; accident or greed.
- **Rationalization** – The most common justification of long-term employees who steal is "I'm just borrowing." Employees who believe they have been treated unfairly can easily rationalize stealing.
- **Opportunity** – The perception someone can borrow or steal and not get caught.

The only element the employer controls is opportunity. To mitigate risk, employers must reduce the perception that a trusted employee can "borrow" from them and not get caught.

Three conditions create opportunity: implicit trust, concentration of duties and lack of oversight. Any one of these conditions creates opportunity for theft, but risks can be reduced if the other two are covered. The existence of all three creates a perfect storm because employees perceive little risk of being caught.

"There was nothing that showed this individual was a potential risk at time of employment," said a MGMA research respondent.

"Circumstances in her personal life led her to make an inappropriate decision, and she thought she would be able to get away with it. It was hard to believe that someone you hired, trained and trusted would do this."

Are smaller groups more vulnerable to loss?

In the ACFE report, the median loss for small business (defined as fewer than 100 employees) in the United States was $150,000 compared to $80,000 for companies with more than 100 employees.[5] Almost three in four of the cases in the MGMA research with a loss of $100,000 or more were from groups of 10 or fewer physicians.

In small medical practices it's difficult to prevent one person from controlling an accounting transaction from beginning to end so oversight — random tests of compliance with established procedures — is the best deterrent. This internal control was lacking in more than 65 percent of the medical groups that were victims of embezzlement.

Risk management is fundamentally about trust. How can you deter the 80 percent of your employees who would steal if they have a need, could rationalize it and believe they will get away with it? Minimize opportunity and institute checks and balances.

"You let teachers and babysitters watch over your children, but you wouldn't expect them to raise your child. It is the responsibility of the owner to watch over the well-being of the practice," said one respondent.

Risk management is a three-step process that encompasses a new best practice: Trust but verify.

1. Assess high-risk areas (co-pays, mail receipts, disbursements, patient refunds, payroll);
2. Segregate duties to the degree possible; and
3. Create a perception of detection by monitoring employee work and testing compliance.

Assessing risk

Evaluate policies, procedures and processes to identify gaps in the system of checks and balances. The internal control checklist on the MGMA Web site is a good place to start. Go to mgma.com/lessons for more information.

A comprehensive risk assessment should be done every year or two and whenever there is a significant process change, such as EHR implementation, the creation of new positions or downsizing.

see **Theft**, page 42

Type of Scheme	MGMA - cases	MGMA - percent	ACFE - percent**	Examples
Cash receipts	335	44.7%	24.3%	Stealing cash either before or after it is recorded on the practice's books
Cash on hand	73	9.7%	12.6%	Stealing cash, such as petty cash, kept on hand at the practice's premises
Disbursements	134	17.9%	42.4%	Forging or altering a check, submitting invoices for fictitious goods or services or from a fictitious vendor, submitting or approving inflated invoices, submitting invoices for personal expenses
Expense reimbursements	27	3.6%	15.1%	Submitting fictitious or inflated business expenses
Payroll	46	6.1%	8.5%	Creating a fictitious employee, unauthorized bonuses or inflated pay rate or hours
Noncash	56	7.5%	16.3%	Stealing or misusing practice's noncash assets such as supplies, equipment or patient financial information
Other	78	10.4%		Respondents reported thefts involving multiple schemes, patient refunds, billing schemes, identity theft, related party transactions, prescription theft and co-worker theft

**In the ACFE column, the total exceeds 100% because a single case of theft in the research can be described by multiple schemes. In comparison, in the MGMA research a single case of theft can only be described by one scheme.

Segregating duties

If one person takes co-pays and can cancel appointments or write off accounts, how would management know if he or she pocketed some cash and deleted or covered up the transaction?

"Separation of duties is critical even when employees are trusted," said one research respondent. "This would have removed temptation for the employee, who began embezzling when her husband lost his job."

Similarly, if one person does the purchasing, approves and adds vendors to the accounting system and signs checks (or gives them to someone who never looks at supporting documentation), how easy is it to set up a fake vendor and invoice the practice for medical or office supplies?

Since it can be hard to separate duties in small medical groups, use other controls to discourage aspiring embezzlers. One option is to create a perception of detection.

To accomplish this, practices should perform routine reconciliations and surprise audits, focus on the tone at the top (the culture of the practice and the attitude of the leadership toward ethical behavior) and train employees to identify and report suspicious behavior.

Routine reconciliations – Reconcile receipts per the billing system to revenue recorded in the accounting system and to bank deposits. The bank statement and merchant card statements should also be reconciled monthly by someone who is not processing receipts or disbursements and cannot process credit card refunds. If this isn't possible, ask a physician or outside consultant to review original bank statements, canceled checks, check registers and supporting detail.

Surprise audits – Conduct unscheduled audits. It isn't necessary to regularly review every transaction or process. It's just as effective to intermittently review specific areas as long as employees know their work will be reviewed, do not know when the review will be done and do not know what data will be reviewed.

In the ACFE survey, victim organizations that used surprise audits suffered significantly lower losses (51.5 percent less) and detected schemes sooner (average duration was 37 percent lower).[6]

Code of conduct – This document should clearly and simply describe your expectations and include where and how employees can seek advice when faced with potential wrongdoing. Have employees sign the document when they are hired and annually thereafter. Adopt a zero tolerance policy for fraud and employee theft of all kinds, and recognize employees who exemplify the spirit of the practice's code. Medical group leadership should be positive role models for ethical behavior and integrity.

High dollar thefts

Amount stolen	Total amount stolen	Percent of total	MGMA cases	MGMA percent	ACFE percent
Less than $1,000	$55,429	0.06%	163	24.0%	2.4%
$1,000 to $9,999	$645,050	0.68%	207	30.5%	7.2%
$10,000 to $49,999	$2,857,800	3.02%	134	19.7%	18.4%
$50,000 to $99,999	$3,320,000	3.51%	50	7.4%	10.6%
$100,000 or more	$87,725,500	92.73%	125	18.4%	61.4%
Total*	$94,603,779	100.00%	679	100.0%	100.0%

* Totals might not sum to 100% due to rounding.

Fraud training – Train employees, managers and physicians on what constitutes fraud, the importance of fraud prevention and deterrence, and how to identify red flags or warning signs exhibited by perpetrators. Fraud hurts physicians, patients and co-workers; it siphons money away from bonus pools and may cause layoffs.

Hotlines – Provide employees with an anonymous whistleblower hotline service to report suspicious behavior. In many cases, employees suspect or know something is going on but say nothing. In both the MGMA and ACFE research, many fraud schemes were uncovered because of tips from employees and vendors or when the perpetrator was absent.

Background checks – In the MGMA research, 62 percent of perpetrators were not prosecuted. Unless a fraud perpetrator has been convicted of a fraud-related offense, nothing will be revealed on a background check even if a candidate has been terminated for stealing.

However, background checks and criminal checks can screen out convicted felons. Be sure to search state and federal court records. Offenders have been known to cross state lines after being released from prison to continue their "trade" in a neighboring state. Once someone has developed a taste for easy, ill-gotten gains, it's hard to pass up future opportunities.

One research respondent advises colleagues to "prosecute, prosecute, prosecute! This administrator had bankrupted other clinics and physicians, but no one had ever stopped him."

Credit checks – Conduct credit checks periodically on anyone in a position of fiduciary responsibility who could override internal controls. Perform a credit check before you hire someone and every year or two thereafter.

Information technology security – Ensure that employees have access only to the programs, screens and data needed to do their jobs. It takes time to develop profiles for each position, but it is an important internal control.

For example, front office staff and cashiers who take co-pays should not be able to write off accounts or delete appointments. If they decide to pocket cash, at least they won't be able to eliminate the evidence. Many of the lower-dollar schemes in the MGMA research involved co-pays and other cash payments, which could have been identified faster if offenders had not been able to write them off.

Trust, but verify

It is important to have trusting relationships, but it is possible to trust too much.

People sometimes make poor choices when faced with personal dilemmas. Physicians and administrators can't be everywhere all the time, and unlimited oversight clearly fails the cost-benefit test. Every practice should establish an organizational culture founded on integrity and ethical behavior that is supported by a system of internal controls.

Notes:

1. 2010 Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, page 4.
2. National Health Expenditures, Table 2, cms.gov/Nation alHealthExpendData/downloads/tables.pdf.
3. 2010 Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, page 69.
4. 2010 Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, page 14.
5. 2010 Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, page 31.
6. 2010 Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners, page 43.