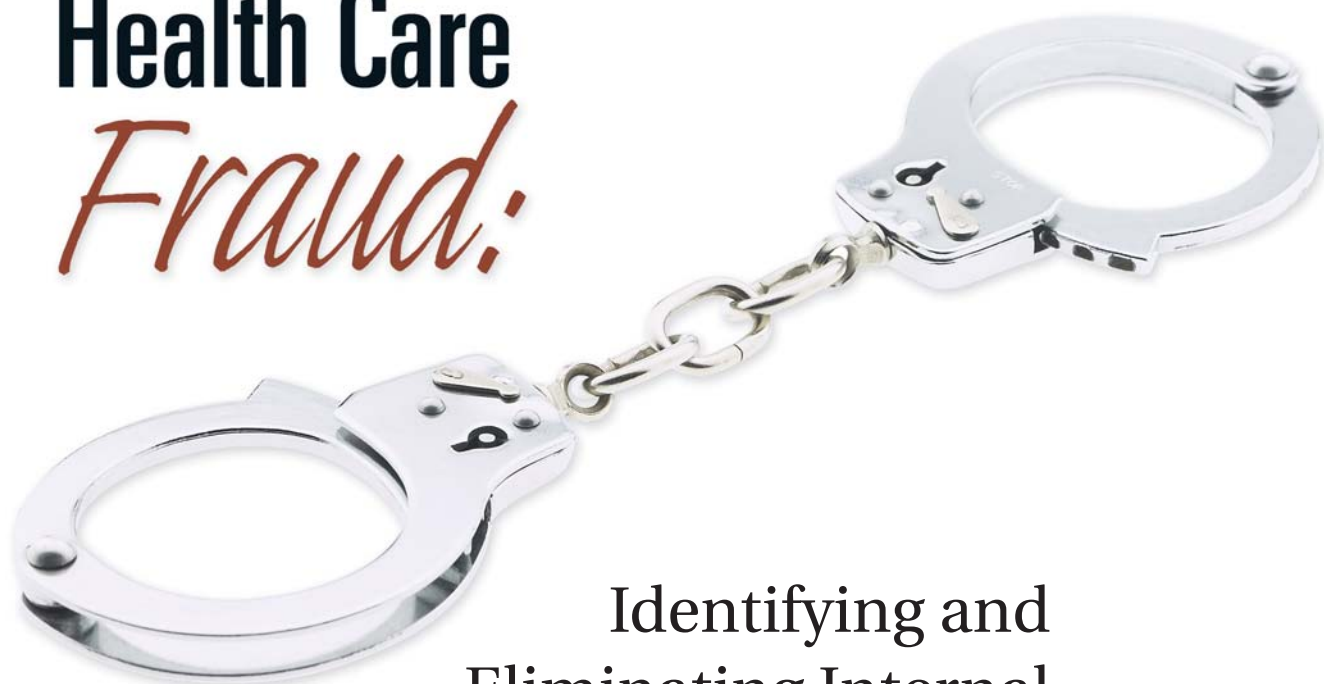


## Health Care *Fraud:*



### Identifying and Eliminating Internal Theft and Abuse

by **Charles Denyer**

©2007 International Foundation  
of Employee Benefit Plans

**F**raud can cause significant loss for a health care organization. By recognizing how would-be fraud perpetrators initiate and conduct fraudulent billing schemes, it is possible to identify, stop and prevent fraud. This article presents significant points to consider when examining an organization's internal accounting systems and offers real-world examples of fraud that have taken place in the health care industry.

*Continued on page 11*

## Identifying and Eliminating Internal Fraud

Continued from page 1

Fraud is the one element people hope never surfaces in their organizations. It can create a culture of fear and mistrust, leading to questions and assumptions, with the ability to severely cripple or destroy an organization's reputation and financial solvency. Most people think fraud would never happen in their companies. Unfortunately, according to a recent report by the Association of Certified Fraud Examiners (ACFE), companies are estimated to lose 6% of their annual revenues to occupational fraud. Just ask Dr. John Doe, whose true story is all too common in the health care industry.

*Dr. John Doe's private medical practice resides in a thriving community in the Midwest. Since 1981, his family practice has seen steady and continued growth, resulting in the hiring of an office manager in 1987. For 11 years, Dr. Doe's office manager, Felix, controlled all financial activities for the clinic, from billing to payments, bank reconciliations, filing taxes and obtaining lines of credit for the clinic's expansion. At the request of his external certified public accountant (CPA), Dr. Doe was told to segregate the duties of his office manager, for fear of Felix controlling too many financial transactions. Dr. Doe scoffed at the notion, stating that Felix was completely capable and in charge, with honesty as his number one motto. Early in 1998, his external CPA questioned the tax return numbers for the past three years, because revenues and expenses were not consistent for his practice. Dr. Doe grudgingly agreed to a small, cursory audit covering invoices for a specified number of years. Confident the findings would be baseless, confirming his feelings and thoughts for his office manager, Dr. Doe vacationed for three days while his CPA conducted a surprise audit on his invoices. And what a surprise to Dr. Doe as he sat motionless in front of his CPA with the results:*

- Since 1991, 13 fictitious companies were established that sent out a total of 147 bogus invoices to Dr. Doe's office.
- These fictitious companies had post-office boxes and other addresses that had direct personal relationships to his office manager.
- The 147 invoices totaled \$85,690.

*• Additionally, seven dummy "doctors" were set up in a health maintenance organization scheme that defrauded Dr. Doe of an additional \$28,000.*

*Though Felix was immediately fired, the damage was so severe that a complete audit of all financial transactions revealed a substantially larger fraud amount due to other improprieties conducted by the office manager.*

Unfortunately, the creation of fictitious vendors and other billing schemes is one of the most common activities undertaken by dishonest employees in health care. And why?

"... It's the perfect crime; from needles to bandages to lab tests and claims processing, the health care industry is awash with an extraordinarily high volume of products, services and transactions moving through different organizations on a monthly basis... the type of health care billing schemes someone can initiate is only limited to their imagination," according to Christopher Nickell, a leading fraud auditor and health care expert. "... A recent audit of three small, rural-based health care organizations consisting of (1) a third-party administrator, (2) a primary care physician practice and (3) an outpatient rehabilitation center found them to have a combined total of 628 vendors on file with a one-month disbursement totaling 1,447 payment transactions for goods and services."

From pencils and paper, to medical supplies, equipment and other miscellaneous items, the list can be extensive and exhaustive. Thus, one can clearly see how this creates an appetite for fraud, which constitutes a staggering amount in losses for health care organizations. According to ACFE, this type of occupational fraud experienced by Dr. John Doe, known as billing schemes, makes up a significant portion of all fraud. So, how can someone identify it and put a stop to it? Dr. Doe's case is typical of what occurs in many health care organizations regarding billing schemes: A trusted employee, who has worked in a position of financial influence, is given considerable control over revenue and expenditure cycles. In essence, he or she controls the funds coming in and the funds going out. Many times, these individuals are simply in charge of purchasing or have partnered with someone, either internally or externally, in assisting them in their scheme.

"... Fraud will always occur where motive and opportunity exist. *Vendor fraud*—vendors colluding with business employees to defraud the business—is one of the most pressing issues for fidelity bond insurance carriers," according to Ryan Caruth, CPA, CFE, a partner in the Atlanta office of RGL Forensic Accountants and Consultants. "This stems from the fact that vendor fraud can be difficult to discover, is easy to orchestrate between a vendor and a business employee, and is very pervasive in all industries."

In addition, vendor fraud typically results in higher monetary losses spanning a longer period than most other types of occupational fraud. Businesses that take a proactive role in establishing and maintaining proper accounting and vendor controls can significantly improve their chances of not being the victim of vendor fraud.

### It All Starts With Accounting Systems

Whether people know it or not, herein lies the answers to many financial concerns—the accounting system. The vendors in an organization's accounting system furnish the keys to unlock and unearth valuable data to ensure fraud and collusion are not occurring. Depending on the size and complexity of an organization, it may be best to use a simple data-mining software tool that will help analyze and evaluate vendor attributes. Easy-to-use data-tracking and reporting applications are often beneficial for finding anomalies in vendor records.

Many health care fraud perpetrators use a variety of activities to conduct fraudulent billing schemes. By recognizing how they initiate these activities, it is possible to identify and stop fraud and, more importantly, prevent it from occurring in the future. There are significant attributes to consider when examining an organization's internal accounting systems, especially the vendors that are used. Each attribute discussed here is followed by a real-world example that unfortunately occurred in the health care industry.

### The Vendor Address

Individuals who commit billing schemes and other related fraud activities need to have funds diverted to other physical addresses. Addresses commonly used are

U.S. post-office boxes and addresses of friends and/or relatives at other types of facilities, such as temporary mail forwarding companies, answering services, and nationwide chains of mail and parcel shops. The post-office box was a mainstay for many years for fraud perpetrators, but the advent of more “traditional-sounding” addresses gave those with the intent to commit fraud a whole new weapon. With that said, be skeptical of addresses with post-office boxes or at mail-servicing companies within a company’s same geographic area.

### Post-Office Boxes

Be especially aware of post-office boxes that have an area code in close proximity to the company. Many organizations in health care today deal with high volumes of mail and use legitimate post-office boxes to handle mail volume; so, more times than not, this is an actual post-office box for a real vendor. Just think of the suppliers that are selling bandages and other disposable goods to clinics and hospitals; their invoicing volume is tremendous, and many times they need a post-office box to handle this volume. However, because billing schemes typically require dollar amounts that can necessitate many invoices, somebody will be making many trips to the designated address. He or she may leave at lunchtime or just after work to conduct the scheme, but the scheme needs to be in close physical proximity, and that’s why vendor addresses close to work are a red flag.

### Other Addresses

As noted earlier, numerous organizations now use mail services, and at reasonable rates. Therefore, a smart move is to be aware of all addresses for known mail-servicing companies within the same geographic area of the company. This list can easily be obtained from the yellow pages or the Internet and is not too time-consuming to review. Remember, time is important to fraudsters; therefore multiple, weekly trips to these addresses to pick up funds may be made, which necessitates addresses in close proximity to the business.

### Actual Occurrence

*A large benefits practice conducted a random vendor audit and uncovered seven addresses that met the criteria just mentioned. Specifically, two post-office boxes*

*within four miles of the company’s office and five addresses recognized as mail parcel and service companies were found. A further investigation ensued, and a fraud scheme that totaled \$24,000 over a 2½-year period was discovered.*

## Employee Address and Other Vital Statistics

Surprisingly, a number of fraud perpetrators actually use their home addresses, vacation properties or other relatives’ addresses when conducting billing schemes. Additionally, they will use either their primary or secondary mobile phones as main contact numbers for fictitious vendors. With only so many addresses and phone numbers that can be used, these people have to “double up” many times, using the same information for a high number of fictitious vendors. An analysis of all vital statistical information can be conducted for employees that are suspected of some type of fraud within a company and compared with vendor statistical information.

### Addresses, Phone Numbers and Fax Numbers

Addresses, phone numbers and even reference information in employees’ personnel files can lead to additional clues. Typically, references come from close friends who just may be willing to use their addresses, phone numbers or some other type of contact information to help aid in the fraud scheme. And remember those addresses from the nationwide mail service providers? They typically allow their fax numbers to be used by customers as their own for purposes of communication. Obtaining those numbers will also be helpful.

Many times, billing schemes will also use a voice-mail provider. Today, voice-mail numbers can be obtained for a very small fee from a number of organizations throughout the country. Vendor phone numbers that sound very familiar but are just a few digits off are a common red flag. Most voice-mail companies buy in bulk, so no matter how much they try to distinguish one number from the others that they sell, similarities can also be spotted if a person knows what to look for. In one particular billing scheme, the auditor noticed that four numbers used for vendors all had the same three-digit prefix but

vastly different numbers for the subsequent four numbers. On a hunch, further inquiry found that the numbers were indeed related to fraud and the billing schemes that were plaguing this particular company.

### E-Mail Accounts

In today’s technologically advancing world, e-mail is one of the most common methods of communication. Fraud perpetrators can set up free e-mail accounts online. Moreover, some traditional, fee-based Internet providers will allow people to sign up without a credit card. Because the e-mail contact address is now an important component of the input field screen within the accounting system for vendors, be wary of e-mail accounts from free services that are used for vendors.

Depending on the degree of suspicion, additional statistical information can be gathered regarding addresses, phone numbers, e-mail accounts and other key pieces of data.

### Actual Occurrence

*A corrugated steel manufacturing company had an internal claims-processing and payment department for its health care plans. The company was self-insured for claims up to \$35,000. Over a 12-year period, the manager of the claims department defrauded the company of \$710,000 by establishing dummy “doctors” who submitted fraudulent medical bills by using the names of employees who actually had very minimal medical expenses during the year.*

## What’s in a Name?

Fictitious invoices can’t be sent and payments can’t be received without company names, so dishonest employees use a variety of schemes for establishing fraudulent, “shell” companies.

### Doing Business As

Obtaining a certificate for “doing business as,” commonly known as d.b.a., is relatively easy. As a result, many fraud perpetrators will use the “d.b.a.” to conceal their real identities and start a shell organization. With “d.b.a.,” it is possible to avoid expensive legal or accounting fees to become incorporated and filling out lengthy state or federal forms. The d.b.a. paperwork, commonly obtained from a

local county courthouse, gives fraud perpetrators a whole new weapon for concealing themselves. With this, they can then open a mail address at any of the previously discussed locations and also open bank accounts.

### Initials

Many fraudsters will use their initials or some other type of common familiarity when requesting approval to use “d.b.a.” Organizations should be suspicious of vendors that have simple initials or odd-sounding names.

### Actual Occurrence

*A vendor billing scheme unraveled at a health care clinic when the mail clerk got suspicious of multiple letters being sent to the company with initials that matched those of the accounts payable manager. Further investigation revealed that this individual in fact used a “d.b.a.” to help disguise her true identity.*

### The Vendor Detail Screen

As noted earlier, because of the high volume of products, services and transactions being conducted in today’s health care organizations, a single entity can have a high number of vendors. Large clinics, hospitals and other service providers in the health care industry can have hundreds or thousand of vendors. Take note of a recent examination of just a small health care organization that uncovered the following vendors:

- 24 vendors for magazine and periodical subscriptions
- 31 vendors for disposable medical supplies and goods
- 14 vendors for outside third-party testing
- 16 vendors for miscellaneous office supplies
- Seven vendors for cost-containment medical consulting
- Four vendors for miscellaneous building maintenance.

Thus, all vendors need to have their updated, current and complete information entered and logged into the vendor detail screen within the accounting system of an organization. If not, there needs to be a valid reason for any omissions, deletions and other questionable data found. As noted earlier, certain information in the vendor detail screen should

prompt suspicion:

- Addresses (post-office boxes, street addresses, etc.) in close physical proximity to the organization
- Vendor e-mails from free e-mail services
- Vendor names with just initials or other suspicious-sounding names
- Phone numbers that sound very similar in numbering and sequencing
- Phone numbers that do not ring and go right to voice mail. They potentially could be nothing more than a voice-mail number purchased from one of many national voice-mail companies.

### Other Red Flags

Many other red flags can raise suspicions that fraud is occurring within an organization. Most people who commit fraud are under some type of financial pressure; but, once these people meet their immediate financial needs, they often continue to steal out of greed. It is important then to watch for lifestyle changes, such as new automobiles, extravagant clothing and expensive jewelry. Additionally, committing fraud will typically result in a system of behavior patterns, beginning with initial guilt, followed by fear and stress, and somewhere along the way a feeling of self-justification that buries or diminishes the guilt.

### Actual Occurrence

*A recent fraud in a large health care organization unraveled as it became known*



**Charles Denyer** is a senior manager with DuPont & Morgan, LLC, an accounting firm specializing in Statement on Auditing Standard (SAS) No. 70 audits and related attestation engagements. His experience includes conducting SAS 70 audits and attestation engagements for third-party administrators, professional employment organizations and payroll companies in the United States and for international clients.

Reproduced with permission from the *Benefits & Compensation Digest*, Volume 44, No. 6, June 2007, pages 1, 11-4, published by the International Foundation of Employee Benefit Plans ([www.ifebp.org](http://www.ifebp.org)), Brookfield, WI. All rights reserved. Statements or opinions expressed in this article are those of the author and do not necessarily represent the views or positions of the International Foundation, its officers, directors or staff. No further transmission of this material is permitted.

*that one of the purchasing managers was known for helping out other employees when they needed small loans for paying monthly bills. Though known internally as “a great person,” “kind” and “giving,” a suspicious internal auditor dug deeper and uncovered multiple instances of billing fraud.*

### Where to Begin

Taking a proactive stance against fraud is one thing, but pointing fingers and making accusations with little evidence is another. It’s important to remember that employees are a company’s greatest asset. Thus, embarking on any type of fraud investigation must be done with great care, discretion and due diligence. Accusing an innocent employee can also have grave consequences for an organization. With that said, if fraud is suspected or if an organization wants to embark on a proactive fraud assessment, the investigation must be conducted in a professional, structured manner. An internal audit department, if the organization has one, is a place to start. The department can help devise a plan and work to find an acceptable approach. Small- and medium-sized organizations that may not have internal auditing departments or employees specifically trained for this type of function might want to consult with an external accountant who has experience in fraud and forensic accounting. **B&C**

*For information on ordering reprints of this article, call (888) 334-3327, option 4.*