10 Ways to Scam a Dentist

And How You Can Avoid Them

by Lisa Horton and Tehra Peace
Dentists Management Corporation

10 Ways to Scam a Dentist

And How You Can Avoid Them

True tales of fraud in dental practices just like yours

By Lisa Horton and Tehra Peace

Dentists Management Corporation

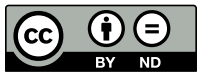


Table of contents

Introduction:
When good employees go bad

Most dental practice staff are good people.

They come to work with a positive attitude. They handle your patients' money and keep your books balanced to the penny. These good, hardworking employees keep your dental practice running, making it possible for you to focus on the profession of dentistry.

Most people are, indeed, good. But we all struggle sometimes, and some of us just can't resist an opportunity when we see it.

In this ebook, we'll tell you real stories about dental practices that have been scammed, defrauded and taken for a ride. All were inside jobs. The common denominator? An employee (or two) who simply got greedy and a dentist without prudent financial safeguards in place. And it's not always who you think.

In many cases, embezzlement is carried out by people who are considered "good employees." They're the first to arrive at work and the last to leave. They almost never take vacations. And why would they? Often their fraud is discovered when they step away from their desks and another employee temporarily takes over — and catches on to the scam.

Much of the time, these seemingly cold-hearted thieves start out as good, honest employees. The first time they steal, it's just too easy, too tempting. They nearly always justify the theft or tell themselves that they'll pay it back. Their fraud usually starts small and just gets bigger and bigger. Finally, the habit takes hold and snowballs, wrecking everything in its path — the dental practice, the rest of the office staff and especially the rogue employee.

Many dentists who have suffered the trauma of embezzlement are terribly embarrassed. They terminate the guilty employee and sweep the fallout under the linoleum. After all, prosecuting the former employee will only bring heartbreak and humiliation to all parties. Because of this, you might hear about only a small percentage of fraud, leading you to believe that fraud isn't as common as it really is. In fact, one in four dentists will be embezzled at some point during his or her career. Embezzlement is a $400 billion per year problem, and the healthcare industry is one of the top six industries affected.[1]

The purpose of this short ebook is to convince you, the practicing dentist, that it is extremely important to have a system of checks and balances in place to prevent fraud. These safeguards can range from high-quality, full-featured practice management software to regular oversight of your books and records. Don't think of these measures as a threat or challenge to the trustworthiness of your staff. Rather, they're a way to protect honest employees.

On occasion, it may appear that your employees are skimming a little — or a lot — off the top, when in fact, they simply don't understand your payment or data entry processes. In these cases, it's just as important to have safeguards in place to ensure that you're not wrongly accusing an employee of theft. As important as it is to have the right systems and software in place to safeguard your practice, it's just as important to train your staff on how to properly use software and accept payments.

Remember, the following stories are true, although we have changed the names and some of the details to protect the innocent — and the not-so-deserving guilty parties as well. These scenarios happen every day in dental practices across the country.

Maybe even yours.

1. "The 2010 Marquet Report on Embezzlement," Marquet International, Ltd., Jan. 11, 2011. http://www.marquetinternational.com/pdf/the_2010_marquet_report_on_embezzlement.pdf

Chapter 1:
Like mother, like daughter

Our first story is a real heartbreaker. Dr. Fields was a nice, young dentist with hopes for the future. He had just bought an established practice that was conveniently staffed with a small group of tightly knit employees. Grateful to have experienced workers at his side to keep the gears running while he learned the ropes, Dr. Fields set to work building his business.

Because the doctor didn't know much about the financials behind his newly acquired practice, he didn't notice when large amounts of cash started to go missing. In fact, his monthly cash receipts had dropped dramatically just around the time he bought the practice. Imagine Dr. Fields hunched over his desk late at night, wondering why his practice wasn't performing as well as he thought it would as he thought it would and beating himself up over where he went wrong.

Meanwhile, in the front office, a long-time employee simply hadn't been able to ignore the lure of cold, hard cash. Debbie wasn't particularly attached to Dr. Fields. He was a newbie and probably didn't understand how hard she worked to earn her keep at the practice.

Earn her keep? She laughed at the idea. She earned more than her keep. Debbie was the face of the practice. She cheerfully welcomed patients every day, scheduled their appointments, encouraged smiles from their fussy children. And when the practice was in a bind and needed extra help, Debbie had even brought in her daughter, Sarah, who had just graduated from high school, to fill a position in the front office alongside her.

Debbie knew she was worth more than what Dr. Fields was paying her. Between the two of them, Debbie and Sarah ran all of the front office activities. They had a monopoly on the practice's incoming cash. Surely no one would notice if Debbie pocketed part of a cash payment here or there. After all, times were tough, and if Dr. Fields wouldn't give Debbie what she was worth, she would make up for it with a little tax-free bonus now and then.

The grift went like this: Debbie would contact a patient with an outstanding balance and tell him that he would receive a 20 percent discount if he paid the remaining balance in full, in cash. When the payment was made, Debbie would post a discount of 60 percent and a cash payment of 40 percent. She would keep the 40 percent difference for herself. So on an original balance of $200, Debbie would stuff $80 into her own pocket and the practice would see only $80. Dr. Fields simply didn't review his reports, so he never noticed Debbie's seemingly generous discounts. Besides, he trusted his employees.

> **» TIP:** *Make sure your practice management software is capable of automatically archiving all receipts (or walkout statements), even if the patient or account has been deleted. In addition, choose software that automatically generates an end-of-day report that cannot be altered, edited or deleted.*

Once she started her con, Debbie could not resist. Things quickly spiraled out of control. Soon, Debbie could no longer keep Sarah in the dark about her activities. She convinced her daughter — still just a teenager — to run the scheme with her.

Over the course of a year, Debbie and Sarah embezzled $37,000 from the dental practice.

It was at this point that Dr. Fields found himself losing sleep at night, wondering where literally thousands of dollars a month was going. He decided to investigate. The revelation broke his heart and shattered his trust.

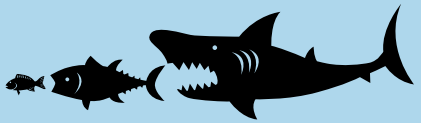
Both mother and daughter were charged with fraud. Because she was young, naïve and following her mother's lead, prosecutors offered to reduce Sarah's charges to a misdemeanor if Debbie took full responsibility for their scheme.

Debbie refused.

As a result of the charges brought against her, Debbie spent two years in jail. She missed out on time with her family — two years of her children's lives.

Dr. Fields and his remaining staff were left to pick up the pieces and find a way to move forward. With a few simple measures in place, Dr. Fields and his practice can catch on to fraud early or prevent it altogether. The right practice management software will automatically archive all receipts for payment and ensure that they can never be removed from the system. As long as Dr. Fields reviews a few of these receipts and check them against his books on a regular basis. He'll then be able to sleep a little easier knowing that his practice is safe.

» TIP: *Practice management software is important, but don't stop at simply installing it. Make sure you and your staff receive full training on how to properly use the software, so that everyone understands the security controls (especially you).*



WATCH OUT: Having the right software is a great place to start, but it's like cruise control for your practice. Cruise control doesn't mean that your car drives itself. Make sure you look at the road (i.e., your records) regularly. Implement strong internal controls in your practice. Background checks on new hires are a must. You also should perform regular financial audits on your accounts receivable system, as well as independent checks on your bank and credit card statements. Remember, just a little bit of effort up front can pay off in the long run.

Chapter 2:
Gone without a trace

It was a normal day at Dr. Gibson's office. The waiting room was bustling with patients, the staff traded lighthearted banter as they worked — it was all the activity you'd expect at a healthy dental practice.

Until the IRS showed up. IRS officers claimed that Dr. Gibson had not paid his taxes. The doctor was in shock. How could this be? Someone must have made a mistake. But now the officers were threatening to put a chain through the practice's doors. Dr. Gibson begged to keep his office open. And then he turned to Dentists Management Corporation (DMC) for help.

Dr. Gibson called DMC because he wanted help pulling information from his practice management software. Maybe he could unearth some clues about what had happened. He also called the local police to investigate.

All this activity was starting to make Jo-Ann, the bookkeeper at Dr. Gibson's practice, pretty nervous. Normally, Jo-Ann was not a lavish woman. She and her husband, who worked part time, didn't make much money, so they lived modestly. For most of her 30+ years at the practice, she hadn't been the type to get noticed and flew easily under the radar.

However, about a year before the IRS showed up at Dr. Gibson's door, things started changing. Jo-Ann began wearing nice suits to work. And one day, she drove up in a rather expensive car. Her colleagues wondered how she could possibly be getting the money. It might be an inheritance, they pondered, or maybe she was just loading herself with debt. In any case, it was impolite to ask these things.

> **» TIP:** *Make sure your software tracks all appointments that are deleted after their start times, as well as all transactions that are removed prior to posting. These entries should be recorded in a log that can't be altered or deleted.*

But now, questions were being asked — about her bookkeeping. The police, Dr. Gibson and the IRS were asking all kinds of questions. Jo-Ann could only sit back and wait, asking herself: Had she covered her tracks well enough?

You see, Jo-Ann had been taking advantage of a flaw in the software Dr. Gibson's practice used. Unfortunately, because the practice was not using software with advanced fraud prevention features, it was too easy to delete information. In addition, the software did not keep a permanent archive of appointments and payments. As a result, neither Dr. Gibson nor police nor DMC could ever prove exactly what had happened, though DMC did find remnants of software on Jo-Ann's computer that allowed her to access the system remotely.

But this is what they think happened:

A non regular patient — let's say someone who broke a tooth while on vacation — would seek emergency treatment at Dr. Gibson's practice. The freshly repaired patient would then pay for her visit in full, either by cash or check. The charges and the payment would be entered into the practice's software, and the office staff would print a receipt or a visit summary.

Later, Jo-Ann would log into the system and delete the emergency appointment from the record, along with the charges and payment. Then, she'd empty the recycle bin. There would

be no evidence left that the patient had ever been seen, let alone paid for the visit. Jo-Ann was then free to pocket the cash or check. The one-time patient would likely never be back to the practice and would be long forgotten by the time billing rolled around. No one would be able to rat out Jo-Ann.

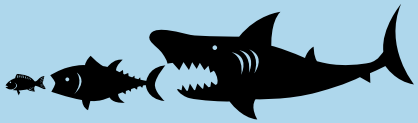
Although they never knew for sure, investigators estimated that Jo-Ann made off with a whopping $180,000 to $250,000 over the course of 18 months.

The police advised Dr. Gibson to map a route between his office and Jo-Ann's home, stopping at every bank or credit union along the way. "Just go inside and ask the teller if there are any accounts in your name that you might have forgotten about," they said. The police also suggested that he could contact his patients and ask them to pull copies of their checks to see where their money had been deposited.

But Dr. Gibson was embarrassed and disheartened. He had already spent so much time and lost so much money to Jo-Ann's inside job. He didn't want to demean himself and his practice any further by exposing to his patients or the bank that he had been "had."

Dr. Gibson fired Jo-Ann. But because he couldn't prove anything, she was never prosecuted. If you ask him today, the thing that angers Dr. Gibson the most is not that he lost hundreds of thousands of dollars; it is that he couldn't stop Jo-Ann from stealing again at another office.

Dentists who want to avoid a scammer like Jo-Ann need to make sure that their practice management software is able to automatically archive receipts or visit summaries whenever they're printed for patients. It's essential that your software also creates a security log of any appointment deleted after its start time, as well as any transaction removed prior to posting. Every dentist — or an absolutely trusted person — should review the practice's security log at least once a week.



WATCH OUT: Embezzlers like to set up bank accounts in both the doctor's and their own name. This setup allows them to stamp checks with the doctor's signature and write the number for the fraudulent bank account on it. They may even have a special stamp hiding in the back of their desk drawer with the phony bank account number! Obviously, the dentist never knows about this account, so con artists are free to withdraw funds to their heart's content.

Chapter 3:
Shop 'til you're caught!

Picture this: You're at your favorite electronics store, and the latest and greatest gadget catches your eye. It has more bells and whistles — and more allure — than ever before. Wouldn't it be nice if you could just swipe your card for the purchase, without ever having the charge appear on your statement?

That's exactly what happens in dental offices across the country, thanks to illicit use of the practice's credit card processing system.

At one practice we worked with, a new employee had a pretty weak work ethic but a hearty shopping habit. This young woman, in her early 20s, had been in the office for about six months. She wasn't invested in the practice, but she didn't mind investing in herself while she worked. She would go shopping during her lunch hour and then, fresh from the mall, returned to her front office job. At her desk, she'd grab her credit card and run it through the practice's scanner as a credit refund, effectively reimbursing herself for her lunchtime purchases. Eventually, her scam was discovered and she was fired — but not before plenty of financial damage was incurred. Sadly, this scam could have been prevented altogether if management had paid more attention to its credit card settlement reports.

A similar but slightly more chilling story comes from the practice of Greater Smiles Dental, where one enterprising employee simply could not resist the temptation to erase her own credit card debt using the practice's credit processing.

Veronica was in her 40s. She was a mother and a faithful, active member of her church. She had been with Greater Smiles for a long time and was a trusted employee. Veronica noticed that it usually took a long time for patients to receive refund checks when they had credits on their accounts. So long, in fact, that no one would notice if those refunds simply never made it to the patients.

Veronica began to target old accounts with long-forgotten credits. Taking the chance that the patient would never resurface and ask for a refund, Veronica would sneak her own card through Greater Smiles' credit processing service and refund the very real credits to herself.

Most likely, Veronica never intended to run her card more than once. But her scam had been easy. Too easy. Once she saw her balance go down, she couldn't resist doing it again and again. Veronica hit the $35,000 mark before she was caught — and it all happened over the course of about 18 months.

One fateful day, a patient called Greater Smiles Dental. He had prepaid the practice for a procedure several months ago, and now he was finally ready to schedule treatment. A front office representative pulled up his account to verify his prepayment, but it wasn't there.

Greater Smiles started to look into other refunds and found account after account with missing money. When the trail led to Veronica, her colleagues at Greater Smiles were floored.

> **» TIP:** *Establish an office policy that you don't do credit card refunds. All refunds must be delivered by check and must be reviewed and mailed by the practice owner. This eliminates those post-shopping-spree urges to erase pesky charges on personal credit cards.*

After all, Veronica had been the last person anyone would have suspected. She was close and friendly with all her co-workers. Her grown daughter even worked at the practice! Imagine her horror when she learned that her mother had stolen so much money from the workplace they shared. But that's the ugly truth in cases like these. Good people find themselves desperate for financial relief and somehow convince themselves that they're not hurting anyone by skimming off the top — even tens of thousands of dollars later.

Veronica's case ends in true heartbreak, as these cases often do. The police arrested Veronica while she was at work, handcuffing her in front of her boss, her co-workers — and her daughter. Veronica was convicted of the charges brought against her and ordered to pay retributions for what she stole. As part of her sentence, she was forbidden from ever again working another job that allowed her to handle money.

Greater Smiles Dental could have avoided fraud like Veronica's by using software that prompts users to make a note as to why refunds are being given. Checking the occurrence of refunds on a regular basis is also an important habit to get into.

» **TIP:** *Only use practice management software that tracks activity by user login to create a permanent audit trail that cannot be deleted. Establish and enforce an office policy for password management and login practices.*

Chapter 4:
Grandmother, what big discounts you give

Betty always had a way of making people around her feel taken care of. She was sweet, nonthreatening and — well, how else can you put it? — grandmotherly. That's probably why she was excellent at her job in the front office at Dr. Garcia's dental practice. And Dr. Garcia liked having Betty around. Whenever the dentist was stressed, Betty would calm her nerves by telling her the same thing: "Don't you worry, dear. I'll take care of it."

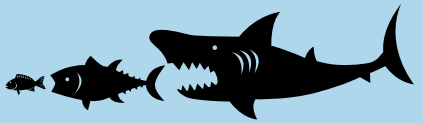
But something wasn't adding up for Dr. Garcia. Her practice offered a 10 percent discount for paying in cash. She also offered a 10 percent senior discount. Why, then, were her practice's books showing 25 percent of her income discounted every month?

Simple. Betty was stealing from her.

When patients came in for treatment, Betty would tell them about the practice's standard discounts. Then after a patient paid for treatment, Betty would post the 10 percent discount she had offered to the patient as a 20 percent discount and keep the difference for herself.

Hurt and betrayed, Dr. Garcia let Betty go. But the doctor didn't press charges. She considered it a lesson learned and just wanted to move on from the incident. Dr. Garcia was lucky that she caught Betty before she made off with thousands of dollars. But Betty is still out there. This sweet, likeable grandmother could be working at any dental practice today.

» **TIP:** *Keep your discounts standard. Make sure that you, and each of your employees, know what the discounts are so that they can never be fudged. Review all adjustment (discount) entries prior to posting, keeping an eye out for unusual items.*



WATCH OUT: Do you have an employee who is the first one in and the last one out? A busy worker bee who never wants to take a vacation or let others help with their workload? They may be more than dedicated workers. They may be afraid to leave their post and be found out. Keep an eye on any employee who seems just a little too willing to work longer hours than the rest of your staff.

Chapter 5:
Signed, sealed, delivered

One day, a dentist called Dentists Management Corporation to ask about our practice management software, DAISY Premier. He wanted to make sure that none of his employees could modify the mailing address for his insurance reimbursements. After we assured him that DAISY restricted access to mailing addresses, we got to hear his story.

His former office manager — a rather bold young man — had logged into the practice's system and changed the mailing address for reimbursements from insurance companies to his own personal P.O. box. After the insurance payments showed up in his mailbox, the employee would pick through the checks and decide which ones to keep. He'd take the rest of the checks into the office and slip them into accounts receivable. He could then delete specific claims from the practice's software, so that the payments he had stolen never had to be posted.

Another common scheme involves an employee changing a name and address for a refund check to his own name and address. After he receives the check, he can log into the system once more and change the patient's information back.

» **TIP:** *Avoid these mail delivery frauds by choosing software that restricts employee access to certain configurations, such as the practice's address. This limits the number of people in your office who can touch this information. In addition, ensure that your practice management software permanently tracks all changes to the billing name and address on patient accounts. Last, but certainly not least, dentists should always keep an eye on payments going out and coming in. Many of these frauds are easy enough to spot, if only someone were paying close enough attention.*

Chapter 6:
Out for revenge

Many of the scammers we talk about in this ebook are troubled individuals, desperate for some extra money to solve their financial problems and convinced that they couldn't possibly be hurting anyone.

In this story, that profile couldn't be farther from the truth. Every so often, an employee will become so enraged with his or her boss that the employee will do everything possible to hit the dentist where it hurts — in the bottom line.

Take Audrey. Disgruntled only begins to describe her. For one reason or another, Audrey was angry with her boss, Dr. Parker. It may have been over salary or maybe Audrey felt that Dr. Parker was favoring another employee over her. Whatever the reason, jilted, angry Audrey decided to leave Dr. Parker's practice. But she was going to go out with a bang.

Audrey looked up the accounts of all her close friends and family members who were patients of Dr. Parker's. One by one, she adjusted their balances to zero and proceeded to delete their accounts. Audrey thought she was really sticking it to her soon-to-be-ex-boss. What she didn't see coming was how her revenge would come back to haunt not just her but her friends and family as well.

Soon after Audrey made her fiery exit, Dr. Parker caught on to her account manipulation. His practice issued new statements to Audrey's family and friends, who, having thought they were off the hook, were now stuck with dental bills to pay. As you can imagine, Audrey wasn't very popular at the Thanksgiving table that year.

This story shows that it's important to have a smoking gun, just in case you ever suspect that a current or former employee has manipulated your accounts. Make sure your practice management software permanently archives all data so that deleted accounts are never completely gone. This way, you can always run a report on the account activity and have a record of who was logged in when an account was deleted.

» TIP: *Ensure that your deleted accounts are never completely gone. Choose software that permanently archives accounts and also tracks user activity, so you always know who did what.*

Chapter 7:
Cash and carry

Here's a scam that happens everywhere, in more dental offices than we'd like to think about. An employee enters a charge for a patient who pays for her visit with cash. Prior to posting the payment, the employee reduces the charge amount and keeps the difference between the original amount due and the amount entered into the system.

An employee can make off with a lot of unaccounted for money this way. This is why you need to make sure that your practice management software tracks any changes made to transaction amounts before they are posted. In addition, you should always protect yourself by having a strict fee schedule and sticking to it!

» **TIP:** *Your software should track any changes that are made to transactions before they are posted. This record will help you see if an employee has charged a patient a higher amount than what has been recorded — or has removed a charge entry entirely — prior to posting.*

Chapter 8:
The bitter end

Dr. Wu and Harriet were more than just boss and employee. They were old friends. Harriet had worked for Dr. Wu for years and years. They had watched each other's kids grow up. Dr. Wu felt lucky to have a trusted friend like Harriet handling the finances for his dental practice.

Every day, Harriet would record all the practice's payments and print a report. She'd write the total on a deposit slip and give it to Dr. Wu. Then, off she'd go to the bank with the carbon copy.

But once she got to the bank, Harriet would fill out a brand new deposit slip — this time, for less than the original amount. She'd pocket a little cash to make up the difference. It wouldn't be missed, because she knew Dr. Wu well enough to know that he never looked at his bank amounts. That was her job.

Eventually, the discrepancy between the amount in the practice's bank account and the number written in its books was large enough that Dr. Wu had to find out where the money had gone. When he finally compared the recorded deposits with the actual deposits, it was painfully clear that Harriet had betrayed him.

Dr. Wu gave Harriet every chance to confess, but she wouldn't do it until he put the evidence right in front of her and threatened legal action. Finally, she owned up.

Amazingly, Dr. Wu did not fire Harriet. Though he was irreversibly wounded and all trust had been lost between the two, Dr. Wu allowed his former friend to keep her job. Harriet continued to work for Dr. Wu until she retired a few years later. But their friendship was gone forever. Dr. Wu learned an important lesson the hard way: It is essential for dentists to compare the deposit amounts from bank statements with the daily reports from practice management software. With a little vigilance, Dr. Wu might have avoided the fraud — and preserved a friendship.

» **TIP:** *You've hired someone to take care of your books for you, so your job is done, right? Wrong! No matter how much you trust your employees — they may even be some of your best friends — make a habit of checking your balances regularly. That way, if there's ever a discrepancy, you can catch it early before it spirals out of control. Even better, never give complete bookkeeping control to one person. Remember, you are the most invested stakeholder in your practice — so stay involved.*

Chapter 9:
In denial

Here's another scam to watch out for. Your trusted employee posts an insurance payment for $0, as though the claim has been denied. In reality, the insurance company has processed, approved and paid the claim — but the benefit check is now going to your wayward employee.

Think your patients will bring this discrepancy to your attention? Not likely. Many of your patients may not understand their Explanation of Benefit statements. Other patients may not even bother to look at them. They're simply trusting your office to do the right thing. That's why your oversight as a business owner is so important.

You still might not think that fraud will ever happen in your office. But as the previous two stories demonstrate, it really could happen to anyone.

» TIP: *Choose software with automatic insurance payment posting so that patients and amounts are loaded directly into the software. Whenever possible, sign up for electronic payments from insurance companies so payments go directly into your practice's bank account.*

Chapter 10:
A mouthful of lies

Sophia was in the past — or at least she pretended to. Every day, Sophia printed reports of the day's activities, which of course, always matched what she gave to her boss, Dr. Weinberg.

But in fact, this tech-savvy con artist had actually changed the system date and time on her computer's operating system to 10 years in the past. This allowed her to enter certain payments into the system and prevent them them from showing up on the daily report. By manipulating the activity date on the reports Sophia was By manipulating the activity date on the reports Sophia was free to help herself to the extra money.

As it turns out, no one can escape time. Dr. Weinberg eventually realized that what he did in production didn't match up to his accounts receivable, and Sophia's scam was exposed. However, just as Dr. Weinberg began the process of prosecuting her, Sophia moved out of the jurisdiction. By the time prosecutors had the evidence, she had gotten away with somewhere between $20,000 and $30,000.

Dr. Weinberg was left with the awkward predicament of having to send new statements and explain to patients what had happened. If only Dr. Weinberg had used software that produced an automatic daily report, Sophia never would have been able to hide payments the way she did. As always, it's vital for doctors to take an active role in safeguarding the financial fidelity of their practices. As you'll see in this next and final story, by catching fraud early on, you can save heartbreak not only for yourself but also for your office staff and even the fraudulent employee and his or her family.

Helen was an office hero. That's because, even in tough times, she always found a way to make sure her co-workers got paid. Helen had started in Dr. Gifford's dental practice as a dental assistant, and 18 years later, she had worked her way up to office manager. The job carried with it a lot of responsibility. Some months Helen would tell the office, "There's not a lot of money in our bank account. We'll have to figure out which bills not to pay so that you can get your paychecks." Her colleagues were grateful to Helen for putting payroll at the top of the list whenever she had to battle the budget, which was often.

As it turns out, Helen had neglected one important rule of budget management: Always pay your taxes, no matter what. So when the IRS showed up at Dr. Gifford's, the practice went straight into red alert.

Dr. Gifford called in Dentists Management Corporation to audit the practice's software. We discovered that Helen had indeed been embezzling from the practice. Like Sophia in the previous story, Helen had also been changing the date on her operating system. When she ran a report on daily activities, her fraudulent entries were hidden in the past and did not show up. However, unlike the other defrauders in this ebook, Helen hadn't been scamming the practice for only a year or two. We traced her fraud back five years. And

> **» TIP:** *Purchase practice management software that automatically archives a non-editable report at each closing that shows the day's starting accounts receivable. In the scenarios described in this story, the starting balance would not have matched the previous day's ending balance, exposing fraudulent activity.*

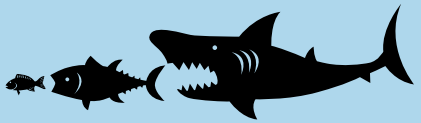
then to 10. Finally, at 12 years, Dr. Gifford told us to stop. “That’s enough,” he said. “I don’t want to know anymore.”

Helen’s actions hurt the practice financially. Because she had completely run the practice’s finances, she had been the only one to see the delinquent notices, which to anyone else would have indicated a real problem. But even more, Helen’s deceit had wounded the entire office staff.

Helen was prosecuted and spent several months in jail. She forfeited her retirement account as part of her reparations to Dr. Gifford. Sadly, the ordeal took a toll on her marriage, and Helen and her husband got divorced. Helen lost nearly everything in her life, and to this day, no one really knows why she did it.

When you consider the risks, it’s hard to understand how anyone in these true stories could have done what they did. Could it have been that the temptation was just too much? That even the best among us, when presented with a combination of personal financial challenges and the right opportunity, would do the same thing?

Some of these stories may be all-too-familiar to you because they’ve happened in your own practice. If you’ve never had to deal with fraud head on, we hope you never have to. Now that you’ve learned from our experiences, you can take action to implement the right processes, software and mind-set to make sure this doesn't happen to you.



WATCH OUT: Don’t ever fall into the trap of giving up control of your practice to someone else. When you let someone else run your finances, they might just run your practice into the ground. You might not like thinking about money, but it’s what keeps your doors open.

Tips

CHOOSING THE RIGHT SOFTWARE

The right dental practice management software is an essential tool for your office. Full-featured software will include security functions that can help prevent or alert you to fraud.

When choosing software, make sure it:

- Tracks all appointments that have been deleted after the start time
- Keeps a permanent, undeletable record of all transactions removed prior to posting
- Automatically archives all receipts (or walkout statements) and ensures that they are easily visible, even if the patient or account has been deleted
- Tracks all changes to the billing name and address on accounts
- Tracks changes to transaction amounts prior to posting
- Maintains a permanent archive of deleted accounts
- Produces reports on activity for deleted accounts
- Tracks activity by user login to create a permanent audit trail that cannot be deleted
- Allows you to set access levels for employees based on their roles and to restrict certain configurations, such as the practice's mailing address
- Automatically archives a report at each closing that shows the beginning and ending balances for the day
- Offers an electronic insurance payment posting feature (sign up for electronic deposits whenever possible so that payments go directly into your practice's bank account)
- Is offered with training and support so that you and your staff know how to use the software and understand its security controls

DAISY dental practice management software provides all these safeguards, while also helping your office run more efficiently. Want more information? Contact Lisa Horton at DMC for expert guidance at 866-252-3976, ext. 3411, or email fruad@dmcdental.com.

THINGS YOU CAN DO TODAY TO PREVENT FRAUD

We can't stress enough how important it is to have a system of checks and balances in place to prevent fraud.

At a bare minimum:

- You must regularly review daily reports.
- No one person should control transactions from receipt to posting to deposit preparation.
- When installing practice management software with fraud prevention features, make sure security levels are set up properly from the start.

- Each employee should have a secret login password; employees should be required to log in and out after every computer use.

If fraud is detected, contact your insurance carrier and the police. Notify patients and their health plans to make sure they have the correct address for claims payments.

LEARN MORE ABOUT DAISY SOFWARE

If you want to sleep a little easier at night knowing that your practice is better protected from fraud, DAISY can help. Featuring DAISY Premier and DAISY Chart, both from Dentists Management Corporation, this full-featured dental practice management system offers all the safeguards and security features we recommend in this e-book. The software's many anti-fraud features were designed with help from a prominent accounting firm that is highly regarded for its consultation services to dental practices. DAISY also includes the latest technology to help your office run more efficiently, while integrating seamlessly with your digital equipment.

DAISY's fraud prevention features include:

- Automatic daily reports that cannot be edited, filtered or deleted
- A permanent record of activity that gives you conclusive evidence if you suspect fraud in your practice
- Advanced security settings that give you control over who can access DAISY, so only certain employees can make changes
- A security log that tracks which computers are accessed, along with the date, time and username
- History reports that tie a username to all additions, edits and deletions for every DAISY entry

To learn more about DAISY software, visit www.daisydental.com. You can also contact Dentists Management Corporation at 800-368-6401 or dmcinfo@dmcdental.com.

ABOUT THE AUTHORS

Lisa Horton has been helping dental offices safeguard their practices for more than 27 years. As an installer and training supervisor at Dentists Management Corporation (DMC), Lisa helps get DAISY dental practice management software where it's needed — into dental practices. She also trains office staff on how to use and get the most out of the software. In addition to her hands-on work inside dental practices, Lisa also contributes to DAISY's ongoing development by serving as the "voice of the dental office" when DAISY's product development team comes up with new features for the software. Her decades of experience give Lisa a huge advantage in helping dental offices operate more efficiently — and more intelligently.

Tehra Peace is a freelance writer based in Portland, Oregon. When she's not writing about the benefits of DAISY, Tehra produces case studies for Fortune 50 technology companies and other communications for major telecom and technology clients. Contact her by email, via LinkedIn or at www.tehrapeace.com.

ABOUT DENTISTS MANAGEMENT CORPORATION

Dentists Management Corporation is located in Milwaukie, Oregon, and supports hundreds of dental providers across the nation. DMC first launched DAISY dental practice management software in 1982 and has continued to revise and improve the software for modern dentists ever since.

In addition to DAISY, DMC also offers complete computer and networking solutions that are tailored to each individual dental practice, guiding dentists through issues such as data storage and security. DMC also provides expertise for integrating digital imaging equipment and software into dental practice systems.

Dentists Management Corporation
10505 SE 17th Ave.
Milwaukie, OR 97222
800-368-6401

www.daisydental.com

SPECIAL THANKS

DMC would like to thank Fluence for its help in creation of DAISY's advanced fraud prevention features. Fluence's knowledgeable consultants guided DMC in our development of the control systems and procedures for DAISY. The organization's expertise and advice has helped make DAISY the most advanced fraud prevention software on the market.

With decades of experience in the dental industry, Fluence consultants help practice owners realize their long-term personal, financial, and business goals. To learn more about Fluence, visit www.fluenceportland.com.