Red Flags and Risks:

Unpleasant Surprises When An Office Manager Suddenly Leaves

By David Harris
CEO, Prosperident

Sure, people leave a practice for any number of perfectly legitimate reasons. But sometimes it pays to be a little suspicious. Especially when an office manager departs unexpectedly. It could be you've just become one of the 50% of dentists who are victims of embezzlement.

Sooner or later, every practice owner receives the unwelcome news that their office manager, who is key to the smooth functioning of the practice, is leaving. If you're that practice owner, a thousand thoughts race through your head. *Where will I ever find a replacement? How can I replicate the amount of knowledge that will vanish with the incumbent? Why is this person leaving us now?*

Many practice owners fall into the trap that, when they find the perfect office manager, they assume that person will be *in situ* forever. Cross-training other staff members never seems like a priority, nor does documenting what the office manager knows and does, or how it's done. Renowned consultant Chuck Blakeman talks about how the "tyranny of the urgent" often displaces the need for practices to undertake longer-term planning. A good time to get such documentation in order is well before your office manager gives notice.

Consider the "why"

In the sudden urgency to replace a key person, one thing that often gets overlooked is to consider the departure circumstances. At Prosperident, we consider ourselves "professional cynics," and are inclined to look a bit more deeply at someone's departure and ask what information might be missing.

(Continued on Page 38)

Embezzlement

(Continued from Page 37)

Sometimes people quit for identifiably good reasons — their spouse took a new job in another city, or your office manager was offered a job with much more responsibility and pay. At other times, the move seems to be "lateral," or the reasons provided seem a bit spurious. Taking a new job because "it's a couple of miles closer to home" is an example of where the person leaving is probably not giving you the whole story.

If you sense that the person leaving is not being candid with you, there can be several reasons. They may be unhappy in their job, which could be the result of a toxic co-worker, or maybe you're a difficult boss. Understandably, many people leaving for these reasons prefer not to be specific.

Another possibility is that they're running away from the trouble they feel is about to catch up with them. Embezzlers who think they're about to get caught will often "do a runner," where they get away from their practice as quickly as possible. So, this is a great time to ask yourself if there has been any event that might give someone who is stealing a reason to fear getting caught.

Examples of things that can frighten a thief are a looming audit by an insurance company, or your spouse becoming more involved in your practice. The change that can strike fear into any embezzler is that you've hired a consultant who is about to start working with your practice. Embezzlers are scared of consultants for a very simple reason — a thief knows your habits and what you scrutinize in a practice, and has undoubtedly planned his or her embezzlement methodology to evade your scrutiny. However, the embezzler has no idea what the consultant might examine. This uncertainty, plus the fact that many consultants are hired to focus more on the practice as a business entity than the practice owner can, creates an extremely dangerous environment for an embezzler.

Almost every consultant has a story about how they stumbled across embezzlement in a practice. It often takes the form of an employee who quit more or less concurrently with the consultant coming in to the practice. So — whenever an office manager or other key employee quits proximate to changes in the office, practice owners need to ask themselves whether there is more to the story.

Account ownership issues come to light

The departure of an office manager often brings to light account ownership issues that can prevent the practice owner from accessing the business's information. And, if a dentist suspects embezzlement may be occurring, being barred from accessing account information makes it difficult to stealthily investigate activities. Examples of how this may occur include the following.

Personal email accounts are used. The office manager may use an individual Gmail account, such as managerfriendlydental@gmail.com, rather than an email account associated with the office's domain, such as suzy@friendlydental.com. But in Google's eyes, it's the departed office manager who is the "owner" of this account. Google has no procedure for the business owner to assert ownership over an individual email account, no matter what its name or how it has been used.

It's certainly tempting to make use of free and easy-to-set-up Gmail addresses rather than involve your IT company to set up your domain-based email. However, as one of our clients found out the hard way, the practice does not "own" these non-domain email addresses, whereas with domain-based email, you can revoke someone's access or have a mailbox redirected to a different user with ease.

Merchant account issues. Another ownership issue that we encounter frequently relates to "merchant accounts." When a practice accepts payment through credit cards, it establishes an account through a merchant service provider. The account is created in the name of the practice it serves, and the merchant service provider has the name of a "contact person" on file.

(Continued on Page 40)

Embezzlement

(Continued from Page 38)

For many embezzlement investigations that we do, we want to review activity in the merchant account to look for fraudulent transactions. Picture a situation where the office manager is under suspicion, but she is also the sole contact for the merchant account. If the monthly statements from this account are under the control of the suspect, the dentist, who wants to keep our investigation covert, will not want to go to this person to ask for monthly statements that they have never wanted to see before. And you cannot get copies of statements from the merchant services company unless it receives authorization from the office manager. In fact, its protocol may be to call the contact (your office manager) to relate that another party tried to access "their" information. Being unable to access a key piece of information needed for an embezzlement investigation is a problem, and the possibility of our involvement being revealed to the suspect because they receive a call from the merchant service provider is potentially a bigger issue.

Contact vs. account owner

Many online financial accounts, including merchant accounts, normally have the ability to provide for multiple contact people. The terms may vary slightly, but often there is provision for both an "account owner" and an "administrative contact." The problem that we are seeing with some frequency is that in many cases there is only a single contact person listed on the account, which makes them both the owner and administrative contact. Since many of these accounts were set up by a team member, it may not have occurred to them to list the practice owner as the "owner" contact. In fact, many dentists even *discourage* having themselves listed to shield themselves from receiving monthly statements and marketing emails that they would prefer not to deal with.

Financial companies are not being difficult by enacting these policies; they are needed to prevent identity theft, which is a rampant problem. Every business needs to take precautions to ensure that it is not taking instructions from an identity thief. Unfortunately, this level of caution, when combined with the propensity of dentists to take little interest in non-clinical activities, can produce problematic results.

Do these things now, before your office manager quits

Your action step is to review the accounts used by your practice and to get yourself added as owner or a secondary contact for any "mission critical" business relationships. Obviously, this is far easier to do before you need access to these accounts in an adversarial situation.

Some of the accounts that should be reviewed to ensure that you have owner-level access are listed below.

Bank accounts. To their credit, banks have handled the difference between owner-level and staff-level access very nicely. If a staff member needs online access to your bank account, rather than sharing your login information as many dentists do, you can set them up with a more limited access that will allow them to check balances and verify if an item has cleared without having the ability to transfer funds or create new bill payees.

Merchant accounts. See above.

Social media accounts. When a disgruntled ex-employee controls a social media account, very bad things can happen.

Practice management software. Ensure that you have full access to your PMS and that employees have only the essential rights to view and edit records.

Domain registration. Imagine firing someone who has the sole control over your practice's domain name. This person could shut down your website. Often, domain registration is done by your IT company, who make themselves the contact. This approach is fine, but you also need to be listed as a contact in case the IT company goes out of business.

Supplier accounts. Every supplier should have you listed as the business owner.

For some practices, account ownership issues may be completely innocent and a matter of convenience, while for others, blocking the business owner from accessing mission-critical accounts may be strategic and indicative of employee wrongdoing. In either case, not claiming ownership of your financial data and communication platforms is asking for trouble. ●

About the Author

David Harris is CEO of Prosperident. His team includes more than 20 highly specialized fraud investigators, forensic accountants, IT specialists, and support staff. He is a sought-after speaker and author of *Dental Embezzlement: The Art of Theft and the Science of Control*.

He is a Certified Fraud Examiner, a forensic Certified Public Accountant, and a licensed private investigator.

Harris