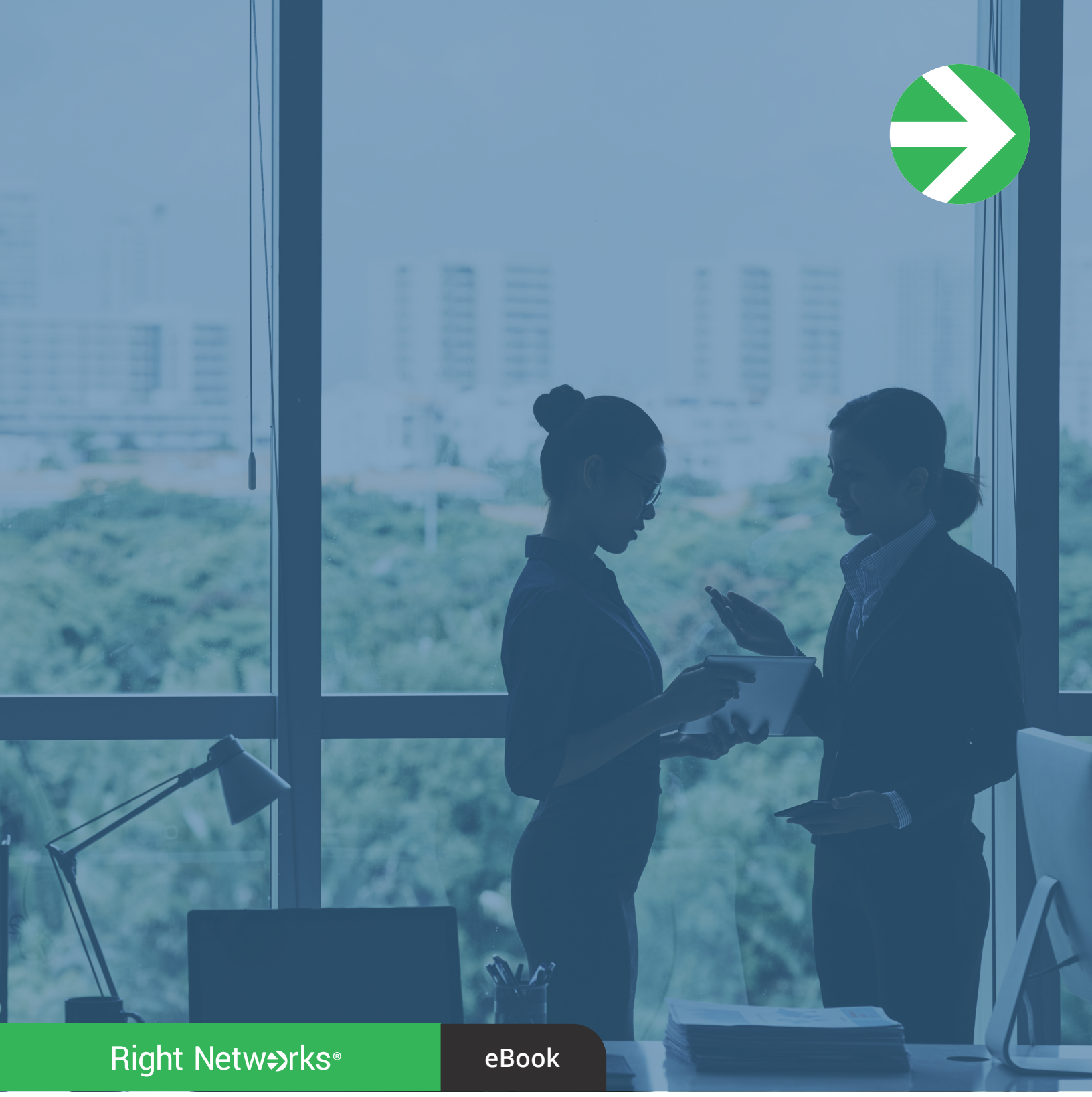


Right Networks®

eBook

How accounting firms can guard against (and even profit from) **employee fraud.**

How accounting firms can guard against (and even profit from) employee fraud.

Accountants know all about fraud. They're trained to spot and avoid it with clients. Some CPA firms conduct audits for other firms in part with the aim of detecting and quashing fraud.

But are firms doing enough to prevent fraud inside their own businesses?

And how can they turn their own fraud prevention into a profitable service?

Those are new questions firms should answer about an old topic.

CPA firms, by necessity, spend a lot of time focusing on cybersecurity, primarily working to prevent attacks from outside the organization. That type of vigilance is critical, but it doesn't remove all threats to the firm's security. Employee fraud remains a threat for businesses of all sizes, firms included.

NUMBERS BEHIND EMPLOYEE FRAUD

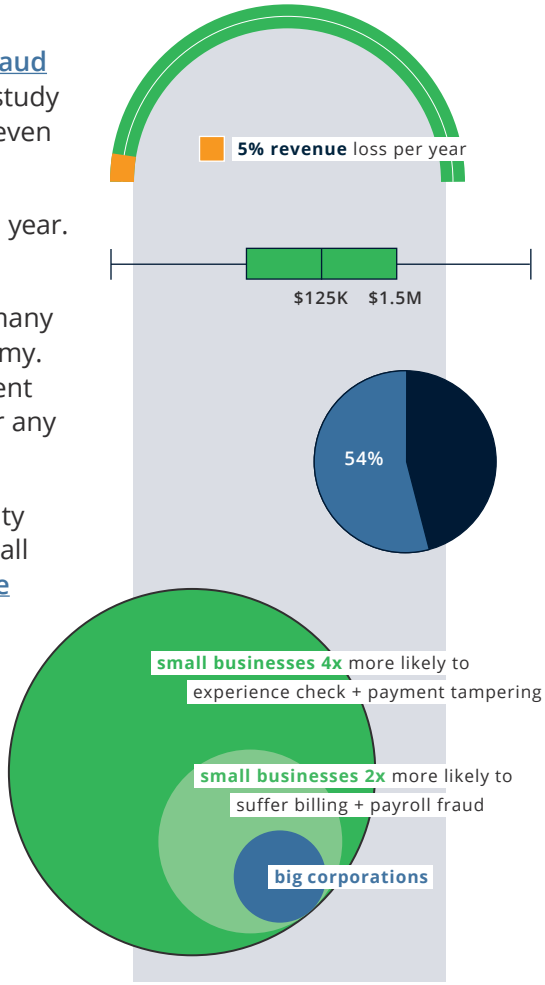
It can be a very expensive problem. The Association of Certified Fraud Examiners' 2020 Report to the Nations, the most comprehensive study of employee fraud available, lays out a scenario that should cause even the most cautious firms to review their anti-fraud policies.

Organizations lose an estimated 5 percent of revenues to fraud each year.

While that might sound like a small number, it adds up to a median loss of $125,000 per case and an average loss of $1.5 million. Not many businesses can afford that sort of hit, particularly in a fragile economy. And once that money is gone, it's very likely gone forever—54 percent of companies surveyed in the Report to the Nations did not recover any money lost to fraud.

What's more, those are losses just from fraud, not from other activity such as cyberattacks or disasters. And the situation is worse for small businesses, including small accounting firms, which are much more likely to be targets of fraud than are big corporations. In fact, the Report to the Nations shows that small businesses are twice as likely as larger companies to suffer billing and payroll fraud and four times as likely to experience check and payment tampering.

Of course, one of the most significant costs of fraud is the damage done to a firm's reputation. After all, accounting firms are supposed to be watchdogs for their clients. What happens when they don't have their house in order? While public examples of employee fraud at firms are relatively hard to come by, often because firms do all they can to hide them, they do happen.



ACCOUNTANTS AMONG THE MOST FREQUENT FRAUDSTERS

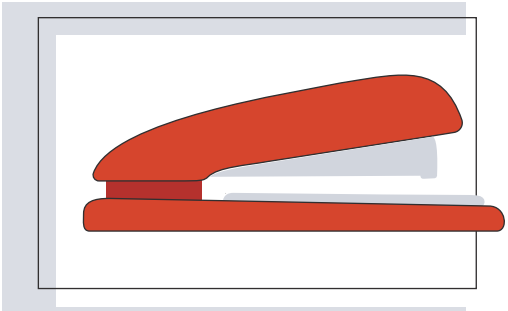
In fact, accountants get themselves into trouble often enough that one accounting website has a regular feature called Accountants Behaving Badly. As a profession, accounting is one of the more likely fields to produce fraudsters. The Report to the Nations reveals that employees in accounting departments were involved in 14 percent of fraud cases worldwide in the time period studied—surpassed only by operations employees at 15 percent.

It stands to reason that people who keep track of money might be tempted to try to misdirect it for their own gain. Some of the other frequent traits of perpetrators of fraud make sense, too. Is an employee who makes $40,000 a year showing up at work in their BMW and strolling in wearing a full-length fur coat? That's a red flag. Is an employee extremely concerned about money, constantly asking for a raise without much justification, or bugging co-workers for loans? Yes, that employee is a potential fraudster, too.

The Report to the Nations confirms that 42 percent of employees involved in fraud cases were living beyond their means—by far the biggest signal that someone is involved in fraud. Also, 26 percent were having financial problems, another development that shouldn't be too shocking. But there are other signs to look for, too, such as an unusually close association with a client (19 percent of fraudsters), control issues or an unwillingness to share duties (15 percent) and even irritability, suspiciousness or defensiveness (13 percent).

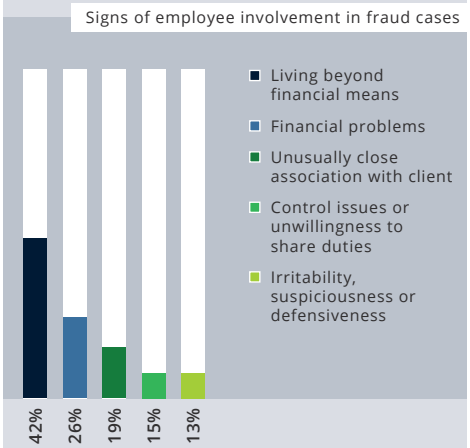
Fraudsters tend to be rank-and-file employees (41 percent) rather than managers (35 percent) or owners of businesses (20 percent)—although owners do by far more damage than anybody else, with a median loss to the organization of $600,000 compared to $60,000 when employees are involved. What fraudsters don't tend to be is new to the organization. Almost half of perpetrators have been with the company for between 1 and 5 years, and the typical fraud case lasts 14 months before detection—although some can go on for decades.

In the movie Office Space, the forlorn protagonists develop a program to skim half-cents off the top of their employer's revenues, but a misplaced decimal point leads to a massive amount of money missing all at once. Unfortunately, while that scenario was great for comedy, it's not common in real fraud cases. Massive gaps in missing cash are rare. Subtle trickles, harder to catch, are more common—and harder to detect.



14% Fraud cases involve accounting employees

15% Fraud cases involve operations employees



TACTICS FOR COMBATTING EMPLOYEE FRAUD IN ACCOUNTING FIRMS

The sad truth is, though, that just about any employee, manager or even principal in a firm can be involved in fraud. Many firms have long-standing practices in place aimed at preventing fraud, and many of those work. For instance, requiring employees to take vacations is still a good way to check on what they've been up to while they're gone. And separating duties—for instance, the same person shouldn't handle both invoicing and post cash receipts—is still a good idea.

The best defense against fraud in a firm, or any business, is still good oversight over financials. That can and should come from inside the firm on a regular basis, but firms should consider outsourcing audits to other firms in a set schedule—say once a year or even every six months. Outside audits eliminate potential conflicts of interest inside the firm, although the less frequently they happen, the more damage a fraud scheme has time to do.

There are other methods of combating fraud that are gaining popularity, though, according to the ACFE's Report to the Nations, and firms that haven't adopted them should consider putting them in place. As the Report notes, a lack of internal controls at businesses contributed to almost one-third of fraud cases over the period of time studied. While outside audits are a necessary deterrent to fraud, they led to detection in only 4 percent of cases cited in the Report. Other methods fared far better in uncovering fraud.

1/3

of fraud cases

were caused by a lack of internal controls

Anti-fraud policy. The Report cites a 13 percent increase in the use of anti-fraud policy over the last decade. While a committed fraudster is likely to steal from a firm no matter what, an official policy serves a few key purposes. First of all, it establishes a legal definition of what the firm considers fraud to entail. Beyond that, it can, and should, encourage employees and managers alike to both look for and report incidents of fraud. It should also specify punishments for employees who commit fraud.

13%

increase in use of anti-fraud policy over last decade

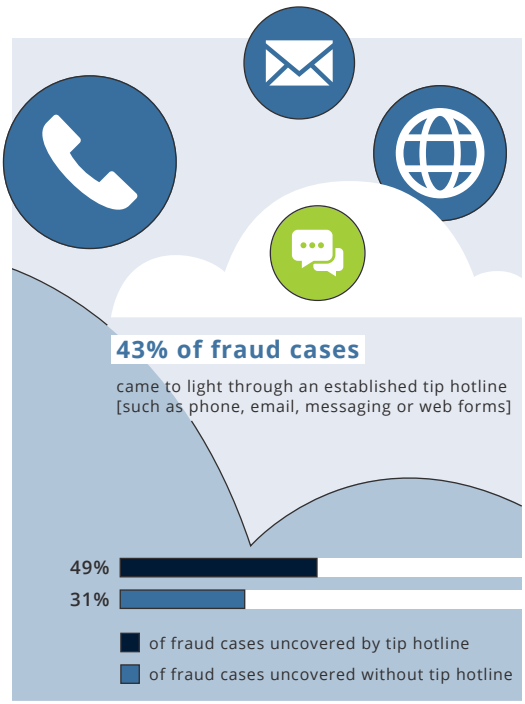
Without an anti-fraud policy, firms could struggle to prove fraud in certain cases, making recovery of stolen money and punishment of perpetrators more difficult. And the concept of codifying employees' responsibility to look out for and report fraud could be critical to catching would-be thieves, as the next point suggests.

Employee and executive training. Training goes hand in hand with an anti-fraud policy, putting into action what the policy sets out about how employees react to suspicion of fraud. Fraud training for both managers and executives is up 9 percent for all businesses over the last decade, the Report to the Nations says.

9%

increase of fraud training over last decade

Organizations with formal fraud awareness training are more likely to get tipped off to fraud by watchful employees than those without it, according to the Report. That's important because tips are the way businesses uncover fraud most frequently. Training, then, is just about discouraging employees, managers and executives alike from committing fraud—in fact, it should focus primarily on how people at the firm should look for and report fraud.



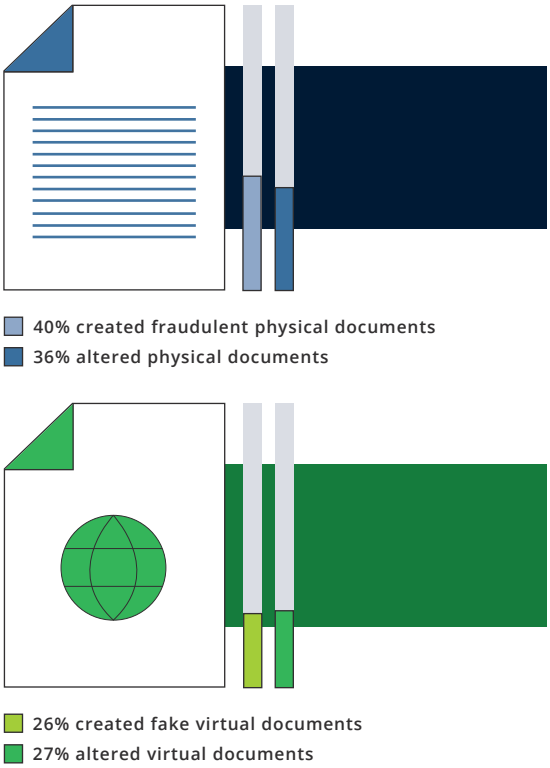
A fraud tip hotline. In the Report, 43 percent of fraud cases came to light through an established tip hotline or some sort, be it via phone, email, messaging or a web form. The next most effective method for uncovering fraud was an internal audit, which was the route to discovery in 15 percent of cases. Tips, and generally tips from rank-and-file employees, are by far the most common way for businesses to detect fraud and reduce both the duration of fraud schemes and the amount of money lost to them.

The presence of a tip hotline flows directly from establishment of an anti-fraud policy and training to back that policy. Training makes fraud detection by tip more likely, and a hotline is also a critical element. The Report notes that in companies with hotlines, 49 percent of fraud cases are uncovered by tip. In those without hotlines, the number is 31 percent. And then there's the bottom line: median losses were nearly double at organizations without hotlines compared to those that had them.

Thorough investigation. Investigating fraud is awkward. There's no way around it. Most employees or managers who commit fraud are not newbies. Fraudsters can include long-time, previously trustworthy employees who steal out of desperation or jealously. A thief can be the person who sits on the corner not saying much—or the person who organizes nights out and keeps everybody laughing. Nobody wants to investigate a coworker.

But the only way for a tip hotline to work is for firms to take every piece of revealed information seriously. Yes, there will be false accusations, so keeping both tips and investigations private is paramount and should be codified in the anti-fraud policy, as should punishments for false accusers. Still, firms need to establish a formal and trusted team to investigate tips, and they need to follow a protocol spelled out in the policy. Obviously, background checks for the team itself should be extensive.

Critical documents in the cloud. In general, the Report to the Nations Reveals, physical documents are a major vector for fraud. The Report reveals that 40 percent of fraudsters created fraudulent physical documents, while 36 percent altered physical documents. By contrast, only 27 percent altered virtual documents, and 26 percent created fake virtual documents. Physical documents are generally easier to fake or alter and pass off. With good controls in place, and with critical business applications running in the cloud, electronic documents offer an added element of security.



The cloud offers other advantages in the battle against fraud. First, firms can track exactly who accesses which systems and which documents, as well as when—providing insight into employees who might show a pattern of accessing certain forms at unusual times or spending more time with a particular form than they should. Backups and archives in the cloud can reveal how documents have changed and when, as well as who changed them. Effectively, the cloud can play a critical role in helping a firm build a case against a fraudster. Furthermore, cloud access records can protect employees and managers from false accusations of fraud, which might be fairly rare but can be devastating.

FIGHTING FRAUD: AN OPPORTUNITY FOR ACCOUNTING FIRMS

While firms need to focus on fighting fraud in their own organizations, they shouldn't ignore the opportunity that combatting fraud for clients can present. Firms that have put in place procedures for effectively preventing and mitigating fraud can use the same tactics to help clients do the same thing. That's not to say that every firm needs to take up forensic accounting, basically the practice of dissecting fraud cases. Just helping put into place a series of anti-fraud measures would provide significant value for many clients.

CPAs are already, by necessity, expanding the breadth of the services they offer clients. Fraud detection and prevention can absolutely be one of them. Accounting firms already take care of the most sensitive information and processes for their clients, and fraud prevention definitely falls into that category. Firms can build on the status they have as trusted partners for clients, and they can offer expertise and credibility that many businesses are unlikely to be able to provide with in-house resources.

Too often, firms fail to understand that the processes they've put in place for themselves can work for their clients as well—and increase firms' revenues in the process. Preventing fraud is an excellent example of just that sort of service. There is even an opportunity to provide outside audits for other firms, a fairly common practice that can serve as a fraud deterrent.

OTHER BENEFITS OF MOVING TO THE CLOUD

The cloud can play a critical role in fraud detection and prevention. But what exactly does moving to the cloud involve? The journey to the cloud is short, simple and inexpensive. First, it's important to know what the cloud is.

What is the cloud, exactly?

Simply stated, the "cloud" is a metaphor for the internet. And, like the internet, the cloud is:

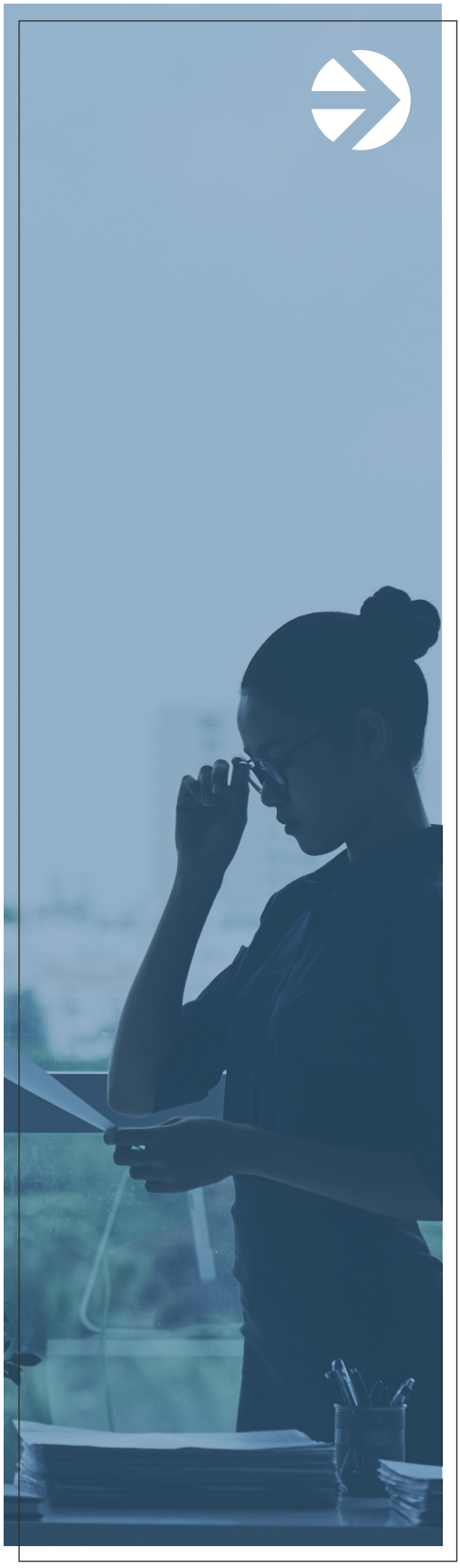
- A place where people go to store information;
- A place where people go to find information;
- Accessible from any internet-connected device, including desktops, laptops, tablets and smartphones.

No matter where firm employees are, if the devices they're using can connect to the internet, they can connect to the cloud. So, when someone says, "My QuickBooks Desktop is in the cloud," what that really means is: "I can open the full-featured desktop version of QuickBooks from any laptop, desktop, smartphone, or tablet."

What does it take to move to the cloud?

Not much, actually. The idea behind moving to the cloud is, in part, to simplify access to critical applications. A move to the cloud is easy. It's really as simple as an email or phone call to sign up for service with a cloud provider. After that, the provider takes care of everything.

- Starting to use the cloud is simple. Once a provider sets up access, all employees have to do is log out of applications once and log back in. That's it.
- The whole move to the cloud takes place off-site, with no involvement from the firm other than signing up for cloud service. The provider's professionals move data to servers in world-class, secure data centers.
- Moving to the cloud doesn't affect software licenses at all. There's no need to get in touch with software vendors or anybody else, for that matter.
- The cutover to a cloud service is nearly immediate and completely painless. It's so quick and seamless that employees probably won't even know it has happened. There is no business disruption.
- And the cloud is not expensive. Moving accounting and business applications to the cloud can cost less than $2 per day.



What are some of the other benefits of the cloud?

- The cloud can be a fraud deterrent, but there's much more to it. The Right Networks cloud offerings deliver a variety of other benefits:
- Access to QuickBooks Desktop, along with more than 250 other business-critical apps, from any internet-connected device.
- Real-time collaboration with clients and colleagues on the same, live, QuickBooks Desktop files.
- US-based support agents trained on accounting and tax application best practices, available 24/7/365.

Plus, Right Networks:

- Is 100 percent focused on accounting and has been for more than 20 years;
- Offers a deep understanding of accounting tools and system best practices;
- Delivers experience in determining the best technology stack to support a firm's CAAS practice.

Fraud isn't going to disappear as a problem any time soon. For accounting firms, having processes, people and technology in place to combat it is critical, and it can even lead to opportunities with clients. The key is to have solid policies and training in place and to stay vigilant, all while employing a cloud system that provides important resources for both eliminating fraud and minimizing its potential impact.