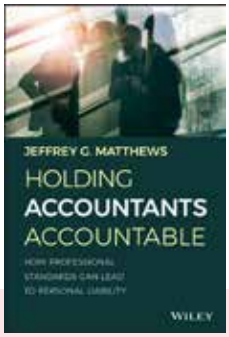
StoneTurn

by JEFF G. MATTHEWS, CFE

ORGANIZATIONS CAN'T AFFORD TO BE OBLIVIOUS. Anti-fraud professionals are trained to be skeptical. They should teach their "trust but verify" skills to all in their spheres. Here are some cases in which the players didn't see (or refused to acknowledge) flaming-red flying flags and paid the cost in **loss of cash and reputations.**



A typical fraud case lasts 14 months and costs, on average, more than $1.5 million, according to the 2020 ACFE *Report to the Nations* (ACFE.com/RTTN). And those are just the cases organizations find. Of course, they fall prey to fraud because they continue to ignore red flags. Failing to investigate can be enormously costly. Witness the MoneyGram case.

On Nov. 9, 2012, MoneyGram International Inc., a global money services business, agreed to forfeit $100 million and enter into a deferred prosecution agreement with the U.S. Department of Justice (DOJ). MoneyGram admitted to criminally aiding and abetting wire fraud and failing to maintain an effective anti-money laundering program. (See tinyurl.com/y76se28v.)

The U.S. government explained that MoneyGram had received thousands of complaints from consumers who were fraud victims, yet the company didn't terminate the suspected agents. The fraud schemes generally involved MoneyGram agents sending elderly consumers false notifications that they'd won the lottery, had been hired as secret shoppers or qualified for loans. The agents convinced the consumers to set up MoneyGram accounts and sent them payments for taxes or processing fees.

The DOJ also claimed that MoneyGram's chief compliance officer failed to ensure the company followed the anti-money laundering provisions required by the Bank Secrecy Act. The language in the act allows for penalties against a "partner, director, officer or employee."

Among other allegations, the DOJ accused the compliance officer of failing to:

- File suspicious activity reports on MoneyGram agents it knew or suspected were engaged in wrongdoing.
- Perform adequate due diligence procedures.
- Terminate relationships with high-risk agents.

The U.S. Financial Crimes Enforcement Network (FinCEN) regulators, a bureau of the U.S. Department of the Treasury, stated:

> The individual failed to take required actions designed to guard the very system he was charged with protecting, undermining the purposes of the BSA. Holding him personally accountable strengthens the compliance profession by demonstrating that behavior like this is not tolerated within the ranks of compliance professionals. (See tinyurl.com/yckp6v9x.)

In 2017, the compliance officer agreed to a three-year injunction barring him from performing a compliance function for any money transmitter and agreed to pay a $250,000 penalty. FinCEN had initially imposed a $1 million fine.

The general counsel and CEO were devastated. They hadn't seen any red flags that would've suggested Bart was a fraudster. However...

In 2018, MoneyGram agreed to an extended deferred prosecution agreement and forfeited an additional $125 million in a settlement with the DOJ and the U.S. Federal Trade Commission. (See tinyurl.com/y7g8e2dv.)

MoneyGram lost millions because its compliance function appeared to be inept, and its accountants and auditors failed to see that the company hadn't applied basic due diligence and the rudiments of the Bank Secrecy Act. Organizations can't say "that would never happen here" until they thoroughly audit their compliance departments.

Controller above suspicion

Even executives who have no anti-fraud or compliance training can teach themselves to pay attention to changing employee behaviors to prevent schemes from continuing.

In 2002, a case of a lifetime found its way to me. The CEO and general counsel of a large oil and gas company called me on a Friday afternoon to tell me they'd discovered an errant fax submittal sheet that had accompanied the transferring of $350,000 for "taxes" from a corporate bank account unknown to them to what appeared to be a personal account at the same bank.

The controller, who'd been with the company almost 25 years, directed the account. He just happened to be on vacation for a few days (which I later learned was also unusual). At that point I realized I'd be working out of town that weekend. I grabbed my project manager and forensic technology professional and drove five hours.

My first meeting was with the company's general counsel and CEO. In the few hours since I'd spoken to them, they'd obtained the bank statements from the corporate account. I determined that more than $6 million in transactions had been processed through the account in the past several years.

The controller (we'll call him Bart) had set up the account and was its only signor. The general counsel and CEO were stunned; they explained that he was one of the most tenured and trusted employees in the company. I found out that Bart:

- Lived in a modest home, which was commensurate with his salary.
- Dressed commonly and drove an older model pickup truck.
- Had been married to the same spouse for more than 20 years and had a teenage daughter.
- Was active with his family in the community and the church.
- Had been with the company almost 25 years, was loyal and never missed a day.

The general counsel and CEO were devastated. They hadn't seen any red flags that would've suggested Bart was a fraudster. They were adamant that he was the last one they'd have suspected. However, after a few long pauses and a handful of questions, they told me:

- Bart didn't socialize with other staff and never had. He was viewed as a loner.
- Bart had recently been using the company computer for personal purposes during work hours. The company had reprimanded him.
- Bart only began using the computer on his lunch hour with his door shut.
- They then noticed his web usage increased significantly. Bart told his

They'd noticed a change in Bart's behavior. He never took lunch and recently always kept his door closed.

CASE STUDY

Don't have faith in the faithless

The CEO of a small, family-owned oil and gas company (we'll call him Jake) is a self-made millionaire. He started his company out of his home, but it grew to a $15 million business in less than 10 years. Jake eventually opened a formal office in a building that also housed one of the state's most prestigious banks. The company's accounting department consists of one person, Anita. She's not a CPA and has little-to-no experience in accounting. But Jake knows her from his church, and he didn't feel a background check was necessary. She has worked in that capacity for the last seven years. Anita is doing such a wonderful job, Jake never hires anyone else to assist her. He's proud that she'd worked out because Anita had a difficult time keeping a job despite her friendly demeanor.

Anita is dedicated to her job. She never takes vacations. And despite a modest salary, she never complains about money or asks for a raise. Jake is impressed because he knows that Anita has helped her mom with her medical bills for the last five years.

Two weeks ago, Anita frantically told Jake that she needed a few days off to help her mom into an assisted-living facility. Of course, Jake approved her request. She said he didn't need to worry about the accounting. Anita said she'd paid all the bills for the business and deposited all receipts. That was good news to him because he hated accounting. He couldn't remember opening a bank statement since he hired her. She'd never felt the need for an audit. He simply hired a CPA to do his taxes each year. Jake was making money, which was most important above else.

Within a few days of her leaving to help her mom move into the assisted-living facility, the bank called Jake and told him that **a check** had been drawn on a dormant, closed account from his business. The bank said the check had been written to Anita for $2,500. The check, which had Jake's forged signature, was the approximate amount of her **biweekly payroll amount**. Jake immediately asked the bank to print out all the checks written to Anita. It appeared that she'd been forging checks for the previous five years and had paid herself in total double her normal salary.

The bank told him it didn't routinely check signature cards, and that the checks payable to Anita had all been prepared manually. All the forged checks had been cashed at a pawnshop.

Jake thought he should sue the bank for not checking his signature card and preventing the forgery. He wanted to testify against the bank that it fraudulently induced him to open the checking account by advertising nonexistent forgery controls.

1. What role did trust play in allowing this fraudulent scheme to transpire?
2. What elements contributed to this trust?
3. What red flags had Jake's company missed when it hired her?
4. Assuming Anita could've passed a background check initially:
   - What pressures might have occurred since to alter her trustworthiness?
   - What opportunities existed for her to commit fraud?
   - How might she have rationalized her behavior?
5. How was this fraud discovered? By accident? By analytical procedures? By a tip? Explain.
6. How would you go about proving Jake's case that the bank should've caught the fraud? How would you defend the bank?
7. What tasks could Jake have performed to have prevented this fraud or at least discover it sooner?
8. How might small businesses be more susceptible to fraud than larger organizations?

10004 102947 10100 1023847

superiors he was day trading. They reminded him that it was still against corporate policy and he must stop. He didn't.

- Then the company restricted his computer access. Bart brought in his own computer and a remote internet connection. The company ignored his actions.
- They'd noticed a change in Bart's behavior. He never took lunch and recently (as I mentioned) always kept his door closed.
- And no, come to think of it, he never took vacation.

How many red flags now can you count? As we imaged his hard drive and began tracing the absconded funds to Bart's personal accounts, we found he was living a secret life. Yes, he was day trading, but he was also placing ads to attract companions. Bart was supporting multiple women. He'd purchased them homes, cars, plastic surgery and even paid for one of their children's education. He'd traveled to exotic locations with some of them.

Bart had an extensive file on each woman, along with every single dollar he'd given them. (Crooked accountants even balance the *second* set of books!)

As we were continuing our computer and file review in his office that Sunday afternoon, in walked Bart. He calmly sat down in his chair and stared blankly at me sitting behind his desk. "You must be the auditors," he said bluntly. "Yes," I replied.

"And I suppose you have some questions."

"Yes. I have many. How did you think this would all end?"

"I always knew I would get caught. I just figured I had another year or two to enjoy things. I know I will be going away for a while, but man, I have had one helluva time."

Bart was right about one thing; he did go away for a while. I learned that his rationalization was a strong desire to beat the system. He was tired of being told what to do, and the computer restriction sent him over the edge. Bart was also in his late 50s, and he felt he'd worked his entire life and had nothing to show for it. He wanted to live a different lifestyle, and this was the only way he could've afforded it.

As unique as this case was, Bart's rationalization wasn't dissimilar to many others. The flags were in broad daylight. Had the company shown the least bit of skepticism, his scheme would've unraveled quickly. But that's the thing: Most of us want to think the best of others, especially if they're part of the furniture.

The flags were in broad daylight. Had the company shown the least bit of skepticism, his scheme would've unraveled quickly.

However, it doesn't take an accountant or an attorney to recognize odd behavior or lifestyle. We must all become skeptics, especially anti-fraud professionals. It simply takes paying attention and exercising diligence when things don't make sense. I've called this tendency "Hey Fever" and "Yellow Fever" ("yellow" as in cowardly). It's the fear of simply exclaiming, "Hey, this doesn't make any sense. Explain."

Sometimes government watchdogs aren't skeptical and objective enough. Government agencies, of course, can be accused of bias missing red flags.

Take, for example, the R. Allen Stanford case. In 2009, Stanford was arrested, and in 2012, he was indicted and ultimately found guilty of running a $7 billion Ponzi scheme. He was sentenced to 110 years in prison (although I bet he won't serve all of them). Many felt the sentence was lenient because he was said to have defrauded more than 30,000 investors in more than 113 countries. The jury found that 29 financial accounts located abroad — worth approximately $330 million — were proceeds of Stanford's fraud and should be forfeited. As a result, as part of Stanford's sentence, the court imposed a personal money judgment of $5.9 billion. (See tinyurl.com/y7f8su8w.)

But that is only part of the story. Questions emerged as to how Stanford was able to keep the U.S. Securities and Exchange Commission (SEC) away so long. In a 159-page report released in 2010 (tinyurl.com/y934hkud), the SEC inspector general found that the SEC examiners in Fort Worth had suspected Stanford was running a massive Ponzi scheme as early as 1997, yet they didn't do anything because of "repeated decisions by Barasch to quash the matter." Spencer Barasch, the former head of enforcement for the SEC in Fort Worth, had gone into private practice in 2005. The report stated the Stanford SEC investigation began "immediately" after Barasch left the agency.

A Reuters investigation, confirmed by the SEC's report, showed that examiners for the agency recommended investigations into Stanford in 1997, 1998, 2002, 2004 and 2005. Reuters stated that in three of those instances, Barasch personally overruled those recommendations. (See "Insight: How Allen Stanford kept the

SEC at bay," by Murray Waas, Reuters, Jan. 26, 2012, tinyurl.com/y7haunub.)

Barasch explained that he made those decisions because he wasn't sure the SEC had statutory authority to investigate the offshore entity, and his superiors had pressured the staff to avoid overly complex matters.

However, in June 2005, Barasch, after he'd left the SEC, sought to represent and defend Stanford and requested permission from the SEC to do so. The agency denied the request and said it'd be a conflict of interest. He asked two more times and the SEC refused both times. However, records obtained during the investigation revealed that Barasch didn't listen to the SEC position and had worked for Stanford.

The SEC inspector general asked Barasch why he ignored the SEC's position. He responded, "Every lawyer in Texas and beyond is going to get rich over this case. Okay? And I hated being on the sidelines."

In January 2012, Barasch agreed to pay the maximum civil fine of $50,000 for a conflict-of-interest charge. The SEC denied him the privilege of appearing or practicing before the SEC as an attorney for one year from the date of the order. Barasch transitioned his practice from the law firm in 2014.

The government never found any evidence that Barasch knew of the fraud at Stanford Financial and never accused him of participating in the scheme. Nonetheless, we can see how challenges to ethical standards could arise. We can see how a career, even one as established and exemplary as Barasch's, can be permanently damaged in a matter of hours.

Don't forget to be skeptics

We all face challenges that test our objectivity and our skepticism. We want to think the best of employees. However, our trust can influence our decisions to pursue investigation, disclose all findings and compile meaningful numbers. Anti-fraud professionals can mitigate their exposure by committing to remain objective, adhere to rigorous skepticism protocols and ethics (such as the ACFE Code of Ethics, and Code of Professional Standards, ACFE.com/ethics) and discharge all assignments with due qualified care. ■ FM

We all face challenges that test our objectivity and our skepticism.

Jeff G. Matthews, CFE, CPA, is a partner at StoneTurn and an ACFE Faculty member. He's a past president of the ACFE's Dallas Chapter. Matthews is the 2013 Certified Fraud Examiner of the Year. Contact him at jmatthews@stoneturn.com.