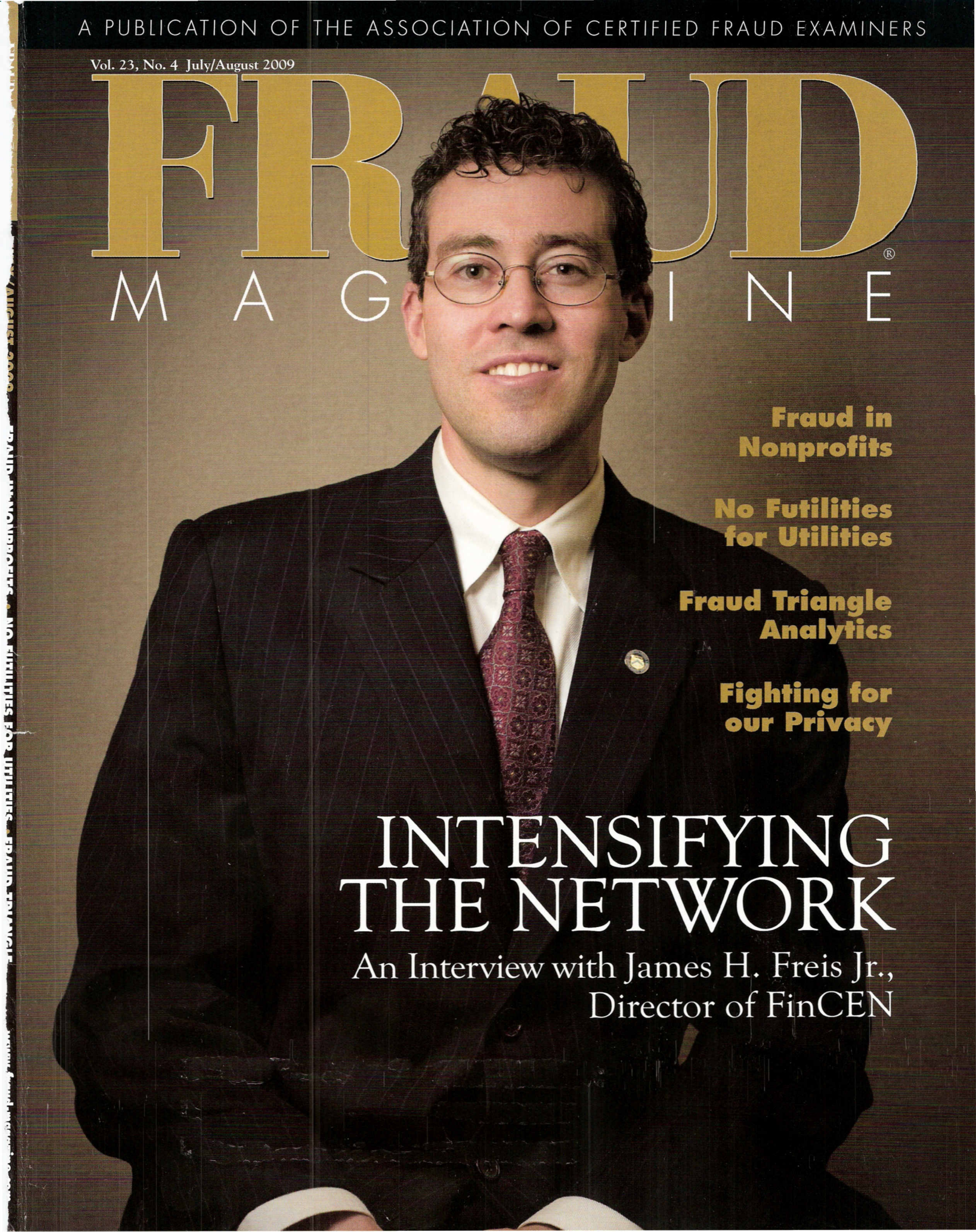
A PUBLICATION OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Vol. 23, No. 4 July/August 2009

FRAUD® MAGAZINE



Fraud in Nonprofits

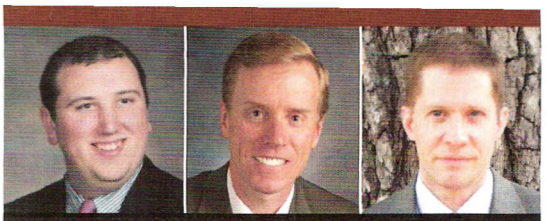
No Futilities for Utilities

Fraud Triangle Analytics

Fighting for our Privacy

INTENSIFYING THE NETWORK

An Interview with James H. Freis Jr., Director of FinCEN



Written by Colin May, M.S., CFE Edited by Mark F. Zimbelman, Ph.D., CPA, Educator Associate Member
Written by Robert L. Bates, CFE, CPA

Preventing Fraud in Troubled Companies

In today's economy, companies are suffering financial losses and diminishing liquidity, which has presented conflicts with their primary lenders.

Our guest columnist is Robert L. Bates, CFE, CPA, president of HP Accounting Services Inc. Read why he became a CFE on page 66.

Economic downturns and recessions are notorious for encouraging fraud. As new and prospective fraud examiners, it's imperative you become aware of the various fraud risks that can occur and the red flags that indicate a fraud in progress.

If you're ever called upon to audit a company or examine its practices to ensure the absence of fraud, you must be prepared to diligently cover all the bases. If you're lucky enough to discover there is no fraud afoot, you still need to quickly take the lead and implement prevention measures to deter any future possibility of fraud.

DESPERATE TIMES

In today's economy, many companies are suffering financial losses and diminishing liquidity, which have presented conflicts with their primary lenders. Banks have come under increased scrutiny, which in turn has increased the pressure on borrowers.

In private companies, owners will feel added pressure to preserve what's left of their companies and livelihood. They will be desperate to stay afloat. When there are extreme creditor/lender pressures, an owner might not see any legal way out of the mess. That's when the environment becomes ripe for fraud.

It's somewhat common for debtors to set up bank accounts at new banks and try to defraud the original lender by siphoning funds to the new location. Debtors might do this for *two* reasons: to defraud a bank outright or to keep a failing business alive. Fraudsters sometimes open accounts out of state or at other institutions where the primary lender won't be able to get its hands on the funds.

DESPERATE MEASURES

During the time when a bank is closing or restructuring a business that has defaulted on its loan, it's quite attentive to the activities and movements of the funds to which it is owed. It might liquidate certain assets or monitor the collection of receivables and new sales to get loans paid back and preserve its secured position as the first debt collector enabled to seek a return on its investment.

Under these circumstances, lenders often hire a firm to either assist the business in restructuring its debt or expense structure (making it into what is sometimes called a "turnaround" company) or performing an orderly liquidation, thus maximizing the recovery on the loan amount.

Some of the tools used are accounts receivable and inventory roll-forwards that track cash, accounts receivable, inventory, and accounts payable. These analyses are different from those performed during a financial audit, and they allow for increased scrutiny of cash. A typical roll-forward shows beginning cash for each period and then classifies all the increases/decreases into functional categories such as receipts, operating expenses, borrowings/paydowns, etc.

The fraud examiner compares certain periods of data to other periods to identify variances and ask relevant questions. An example of something an examiner can look for would be to match receipts against decreases in accounts receivable on an aging report. Underreporting receipts on the books indicates the collections could be diverted elsewhere.

The fraud examiner's job is crucial in preserving the bank's position. Banks require the expertise of CPAs and CFEs in these areas because they're beyond the scope of the banker's expertise and time limitations.

SPOTTING RED FLAGS

I was recently in a situation in which a bank (Bank B) employed my firm to monitor the wind down of a company. Our job was

to collect existing accounts receivable and inventory in an effort to pay off the loan balance. While on site, I reviewed financial records and noticed there were two sets of financial statements within the same accounting software.

The captions on the second balance sheet indicated cash being held at Bank A and Bank B. Bank B is where legal loan documents indicated all transactions should be occurring. Bank A had $85,000 in recent deposits and it appeared the company was using it to divert funds that were supposed to be paying off Bank B's loan. The company's cash records weren't current and months of bank reconciliations were incomplete. These were bright red flags and I knew I'd uncovered a fraud.

This case is typical of the kind of fraud that occurs when a company is in financial trouble. There were some bank examinations performed by Bank B prior to my involvement, but they were minimal and didn't uncover the fraud.

The examination indicated that more than $200,000 worth of accounts receivable money had been collected, despite the lack of documentation or accounting entries to support the claim. The lender didn't even know there was an issue until the company started bouncing checks.

PREVENTING FRAUD

To date, Bank B has only wanted to spend limited funds on investigating the case because it can be hard to prove money was ever diverted in the first place, thanks to the messy bookkeeping and tangled webs of information. The case is still ongoing as final sales continue and collections remain pending. The company owner's house is one of the few pieces of collateral left for the bank to acquire.

Periodic review of the company's financial records and preparation of basic roll-forwards would have indicated the existence

of incoming funds that never made it to the bank and could have prevented the fraud and saved the bank and the company a lot of time and money.

Client's Case Leads to Earning CFE

I've worked as a CPA and controller for many companies in many industries, and I've seen evidence of fraud before. But a client's case in 2008 finally inspired me to learn even more about fraud examination principles. I realized that I needed specialized training to identify fraud in financial transactions. That's why I turned to the ACFE for continued education and credentialing. I became a Certified Fraud Examiner this year.

It's interesting to think that I might never have come down this path if not for a random assignment that resulted in a fraud discovery. I was reviewing the books and preparing financial statements for Company A and a related company, Company B in this particular case. As a colleague and I reviewed Company A's QuickBooks files, my colleague made several general suggestions about various accounts on file. When we got to fixed assets, he pointed out that a payment of $3,000 to the company's bookkeeper, "Betty," should be shifted from ordinary expense to a capital cost because the QuickBooks description said it was for "office improvements," to which Betty shouldn't have any connection.

I verified some tax/year-end entries that hadn't been made into the accounting system yet. While I was reviewing the books for Companies A and B, noting similarities and differences, I began to wonder about the $3,000 transaction in Company A. Something didn't seem right. So I decided to look up entries for Betty in Company B. I noticed she was named in multiple transactions in 2008, each for several thousands of dollars. In prior years there were even more payments to her. It seemed unusual to me for an employee like Betty to be reimbursed so often for transactions that could have been made directly to vendors.

A HUNCH CHECKS OUT

I returned to my office Monday and mentioned my concerns about Betty's checks to another colleague. He also found the circumstances unusual, so we arranged to meet Betty at the client's third office, which housed their accounting files. During the interview, Betty was unable to provide many answers.

Some of the items we asked her about included cancelled checks, invoices, and other irregularities. I was concerned because some of the signatures on checks written to Betty looked different from signatures on other checks written supposedly by the same people. Also, I learned that many employees were given company credit cards; but oddly enough, Betty was the only employee who had the statements mailed to her house.

Things weren't adding up, so we documented what files we could, and copied certain items of significance. Our next discovery that day confirmed our suspicions that something was definitely awry; despite the fairly well-organized filing system, the payables file on Betty were not with the other vendors' files. The fact that it was the only one missing was very puzzling.

INTERVIEW WITH SUSPECT

A few days later we returned to the main client office to ask Betty about various transactions including some related to her and the missing file with backup for payments to her. I noticed several red flags while we interviewed Betty. While I didn't know how much her clothes cost or what her lifestyle habits entailed, I felt there was something too sophisticated about this bookkeeper, who made $50,000 annually.

Every time we asked Betty a question, she referred us back to the accounting software. She also couldn't provide source documents. Even though American Express credit card (AMEX) statements are readily obtainable online, she tried to confuse the situation by claiming she couldn't print the statements. Within days Betty was terminated and accused of embezzlement. Civil and criminal charges were filed.

While putting together the evidence to take Betty to court, I made a spreadsheet documenting all items in question. After accounting for questionable AMEX and Visa charges, her tab totaled nearly $300,000 stolen in four years.

SCHEMES UNCOVERED

It wasn't long before we discovered that Betty used two schemes to steal company funds. She booked credit card expenses of a particular amount and then cut herself a check for a significantly larger figure. For example, a bill would be $2,072 and Betty would cut a check for $7,072.

Details of the stolen $300,000 were documented in QuickBooks. And because it was the primary information source relied upon for auditing purposes, it didn't arouse any suspicion. She'd been able to get away with her fraud for so long because she came up with somewhat legitimate-sounding reasons for the withdrawals. For example, if there was a refund for $5,000, the QuickBooks description might have read: $3,200 travel, $1,800 tickets.

In her other scheme, Betty put her personal expenses on a company Visa card. These were hundreds or thousands of dollars a month for gas, food etc. This bill totaled more than $50,000, but since it was in smaller increments it wasn't obvious in a cursory look at the books.

FOLLOW-THROUGH

I called vendors to clarify vague ledger listings like "Travel package" or "US Air." What I eventually discovered was that Betty had used company money to purchase personal vacations and concert tickets worth tens of thousands of dollars, and there were even some cases in which she just paid herself cash with no receipts or any other type of backup.

I reviewed and documented Betty's and other employees' transactions and sampled several cash transactions. I searched her desktop and laptop computers and went through her e-mails seeking further evidence of ticket purchases and perhaps coercion or collusion, but I didn't find anything concrete to connect her actions with others at the company.

Meanwhile, the company hired a law firm to protect its rights and to investigate Betty's assets so the court process could begin. They got a quick judgment on a recently purchased home and then alerted the police.

Hopefully, Betty learned a lesson about stealing. Eventually things catch up with you, especially if you steal large amounts of money or continue your fraud over a long period of time.

While this case seemed typical at first, I eventually found an intriguing fraud that helped develop my inquisitive nature and led to a more focused career choice in fraud detection and prevention and, ultimately, to my ACFE credentialing. Thanks, Betty!

***Robert L. Bates, CFE, CPA**, is president of HP Accounting Services Inc. His e-mail address is: hpaccounting@comcast.net.*

***Colin May, M.S., CFE**, is a forensic financial investigator with a government agency (the views in Starting Out are his own) in Baltimore, Md. His e-mail address is: camay@officer.com.*

***Mark F. Zimbelman, Ph.D., CPA, Educator Associate Member,** is an associate professor of accounting and Selvoy J. Boyer Fellow at Brigham Young University in Provo, Utah. His e-mail address is: mz@byu.edu.*