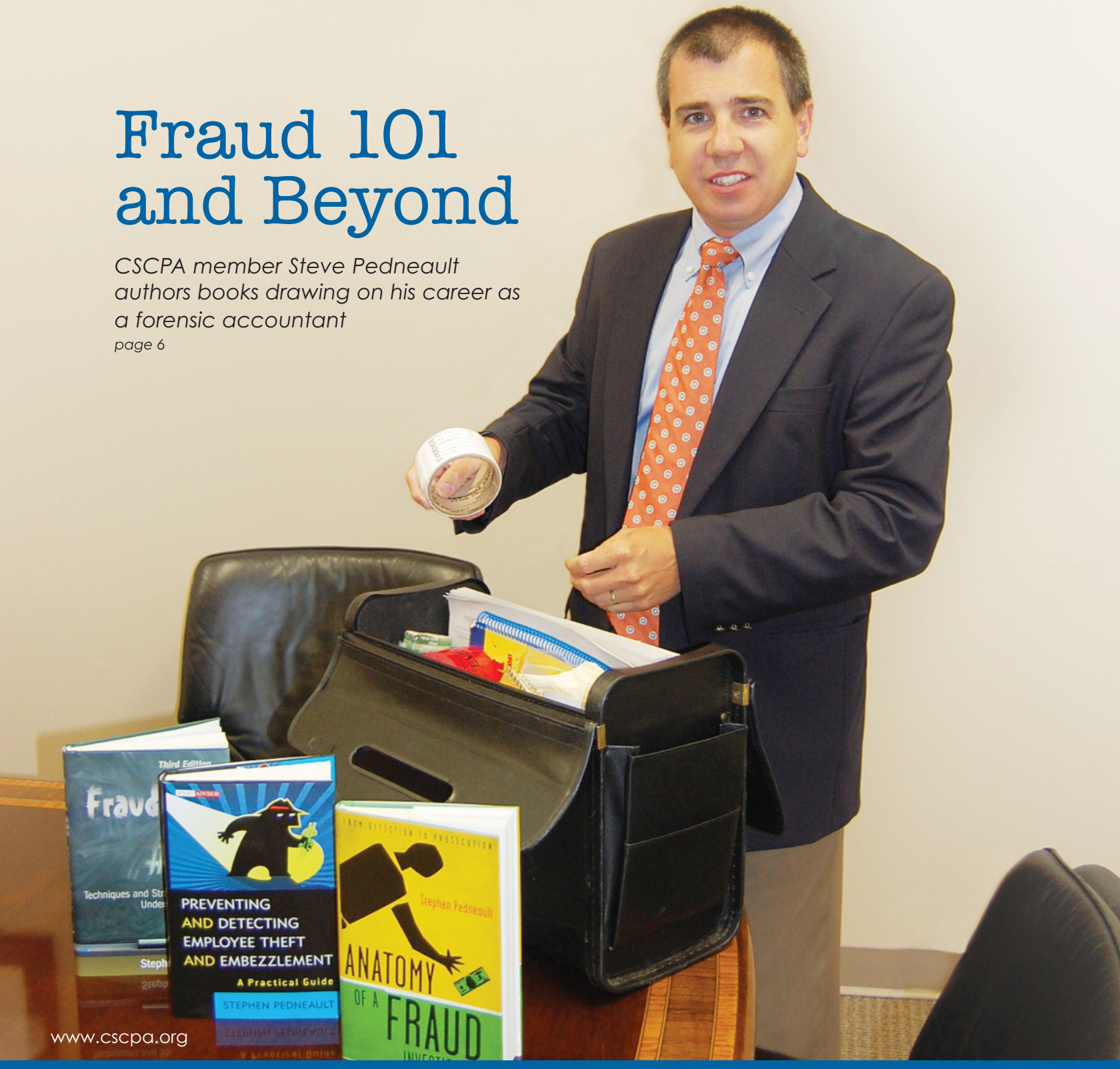
Connecticut CPA
A publication of the Connecticut Society of Certified Public Accountants
Sept/Oct 2010 • Vol. 51 Issue 5

Fraud 101 and Beyond

CSCPA member Steve Pedneault authors books drawing on his career as a forensic accountant

page 6



www.cscpa.org

Internal Controls 2010: Should We Head Back to Basics?

By Stephen A. Pedneault, CPA, CFE, CFF, FCPA, Forensic Accounting Services, LLC

Circa 1988 – the beginning of my accounting career.

The economy was booming … Not really, but doing slightly better than today's, with the late Ronald Reagan leading our country. Personal computers were entering the workplace, with Lotus 1-2-3 and WordPerfect automating ledgers and making typewriters antiquated. The state-of-the-art desktop was an IBM 286 with a 10 MB hard drive and a 5¼-inch floppy drive.

Most businesses were still maintaining their bookkeeping manually, using One Write checkbooks and green columned paper. A software package called One Write Plus, written to automate the manual One Write system, was competing with Peachtree for market share, running on DOS (Disk Operating System). Monitors displayed in color … one color, that is, and it was amber, green, or blue. A special monitor and video card were required to display in true color (RBG).

Monthly bank statements were received in the mail, along with all the actual cancelled checks. Once received, the checks would have to be sorted numerically by check number (and not by amount, as a few of my bookkeepers thought) for ease of reconciling and to ensure all the checks were in fact returned. Credit card merchant statements were also mailed out monthly, identifying not only the activity processed during the month but also the credit card numbers associated with each transaction. Deposit items had to be listed separately on the deposit slip, or at least include an adding machine tape stapled to the slip, and copies were made of everything for the files.

At the end of each month, bank reconciliations would be completed, comparing the checkbook activity to the actual cancelled checks (and not the printed check information provided by the bank on the statement), frequently with the reconciliation completed right on the back of the bank statements themselves. Recurring entries would be recorded, adjustments posted, and once the balances were finalized, reports were generated and the period was closed – really closed, hard closed. With that, the past accounting periods could no longer be accessed or adjusted, and all subsequent activity would have to be posted in the current months.

On This Issue's Cover

CSCPA board member and author Steve Pedneault shows one of his new books to CSCPA President Marcia Marien.

Stephen A. Pedneault, CPA, CFE, CFF, FCPA is the owner of Forensic Accounting Services, LLC in Glastonbury. In recent years, Pedneault has taken his knowledge in forensic accounting and fraud to the masses, writing three books on the subject. *Fraud 101: Techniques and Strategies for Understanding Fraud* was published in September 2009, *Anatomy of a Fraud Investigation* in February 2010, and *Preventing and Detecting Employee Theft and Embezzlement: A Practical Guide* was published in June 2010, all by Wiley.

Pedneault, the 2010-2011 CSCPA secretary, is also active on the CSCPA Valuation, Forensic, and Litigation Support Group and is an adjunct professor for the University of Connecticut master's program.

So what changed?

Technology, banking, software, even where and how bookkeeping is completed has changed over the past 20 years, with changes occurring even more rapidly in the past 10. The return of cancelled checks was phased out by financial institutions and replaced with images, then front images only, and ultimately no images at all. In today's banking environment, the images are often available through the bank's online system to be viewed or printed as needed. Even the bank statements themselves with some financial institutions have been phased out, no longer provided via paper (or provided at a fee), but available any time online.

Deposits can be made today without ever leaving your desk, scanning the deposit items and transmitting images (in some cases the MICR line only) of the deposit items. The bank never takes possession of the deposit items, only a file containing the images.

Mailed monthly credit card merchant statements have become close to extinct, replaced with on-demand online access for viewing and printing, with the individual credit card numbers replaced with transaction numbers if provided at all.

Most software packages used today never require any monthly close, and the ones that do have provisions to re-open a closed period. Packages commonly used like QuickBooks simply continue in perpetuity, from day to day, to week, and to year. Today's accounting systems could be located on an employee's hard drive or laptop at the organization, or at their house, on the organization's file server, or simply out on the Internet ("cloud computing"), where the organization's most sensitive and confidential information is housed on some server in some unknown area of the world being maintained by unknown individuals. The same holds true for many organizations' payroll systems.

Opportunities to divert funds are being created without thought of the potential risks.

So where are we heading?

Today's business climate, in response to the declined economy, is tougher than ever. Streamlining, staff reductions, and efficiencies are all key themes to surviving and maintaining a positive cash flow. With these changes come less segregation of duties and duties once performed no longer being completed due to reduced capacity.

Opportunities to divert funds are being created without thought of the potential risks, and coupled with the high levels of stress, personal financial pressure, low employee morale, and longer work hours, the requisite rationalization can materialize, leading an otherwise honest employee to "borrow" funds from his or her employer.

Despite the downsizing and other changes being implemented, it is critical that basic-level internal controls are implemented and maintained to minimize every organization's risk for employee fraud and theft.

Complacency kills.

In many recent cases, there appears to be a trend where good internal controls

(continued on next page)

existed, but for some reason the individuals responsible for performing these controls stopped doing their reviews, checks, and balances. It has not been uncommon for owners or executives to rationalize their abandoning of performing key controls and reviews because they have "trusted" individuals working for them. Unfortunately, statistically, these "trusted" employees are often the ones who steal from the organization – and in large amounts over long periods of time.

In one recent case the controller was "trusted" to perform virtually every financial process within the organization. Little to no oversight was ever implemented over the controller's activity. Year after year, the controller handled all aspects of the organization's finances.

One day an accidental discovery revealed the controller inappropriately used organization funds for personal purposes. A formal investigation into the controller's past activity and transactions was initiated and, as a result, multiple diversion schemes were identified leading back several years, all of which should have been detected within the first month the controller started inappropriately using the funds. In the end the "trusted" controller diverted more than $500,000 from the organization.

Basic internal controls should have prevented this or, at a minimum, would have detected the controller's activity within the very first month. All of the personal activity was easily identifiable on the monthly bank statements. Someone independent of the controller, ideally the primary check signer receiving and reviewing the organization's monthly bank statement, would have detected the schemes early on and minimized the loss.

In another case, an employee diverted payments received from customers, concealing the thefts by simply posting payments to customers' accounts within accounts receivable. Once the balances were "paid," no further follow-up was performed on the balances, minimizing any risk of detection.

No independent reviews or reconciliations were being performed to compare what was received each day to what was posted as payments daily, and also to the actual bank deposits for the same day. This three-way reconciliation completed on a daily and monthly basis would have identified if differences existed (almost daily) between payments recorded within accounts receivable versus the actual bank deposits.

No copies or images were maintained of the customer payments, preventing anyone from determining the composition of each deposit and further limiting any risk of detection, as there were no means to compare the customers credited with payments to the actual customer checks that were deposited. An independent review of the deposit batch of payment copies compared to the actual bank deposit would have also revealed the theft.

Limitations due to available records prevented us from determining if the employee had been stealing for weeks, months, years, or all the way back to when they were hired 15 years ago.

What can be done?

So many instances of employee embezzlement could have been either prevented or detected had basic manual controls and procedures been implemented and followed. Basic controls would include simple measures like the primary check signer directly receiving the actual monthly bank statement and reviewing it for reasonableness before it is passed along for someone to reconcile.

Every employer, regardless of size and industry, needs to objectively evaluate their financial policies, internal controls, and accounting procedures to determine which basic controls are necessary and appropriate. Basic controls would include the controls recommended back when deposits were manually reconciled and physically taken to the bank, when checks were hand-written and hand-signed for every disbursement, and when payroll was distributed to each employee in person, after careful review to ensure no individual employee was paid (typically in cash) more than they were entitled to receive.

Some basic controls to consider are:

- Each day's receipts should be processed intact daily as a batch, with copies made to support the day's receipts. A report identifying the posted payments should be generated and, together with the bank deposit slip and deposit receipt, should complete each day's batch.

• Someone independent of processing receipts should review and reconcile each batch for reasonableness. For space consideration, each day's batch can then be scanned and maintained electronically.

• Supporting invoices and receipts should accompany every check for signing. Each check should be manually signed and then mailed out directly by the signer, and not returned to the individual who generated the checks. Signature stamps need to be eliminated.

• Petty cash accounts need to be controlled and reconciled by someone other than the person responsible for maintaining the accounts. The same holds true for any client fund accounts, trust funds, or any instances where funds are maintained on behalf of others, ensuring an independent review is completed regularly.

• Individuals with access to add, change, and terminate employees within payroll should be separate from employees who process payroll.

• Payroll should be reviewed before and after transmitting for processing, whether internally prepared or through a payroll service. The payroll package should be received directly and reviewed by someone other than the individual who processes payroll.

• Monthly bank statements should be received in the mail and include images of the cancelled checks, unless the fee to provide the images proves cost-prohibitive. Reviewing the images in many cases would reveal unauthorized disbursements and without the images, other controls will be needed.

Talk to your clients.

Embezzlements are occurring at increasing and alarming rates. Regardless of the level of service you provide, you need to speak with your clients about the risks that may exist

(continued on next page)

"Trusted" employees are often the ones who steal from the organization – and in large amounts over long periods of time.

within their respective organizations and ask them what they are doing to minimize their risks.

For those entities that are audited, our professional standards require the auditor to review and assess the client's systems of internal controls to determine how much reliance can be placed on them, as well as identify and report any deficiencies and material weaknesses. What about non-material weaknesses that are identified?

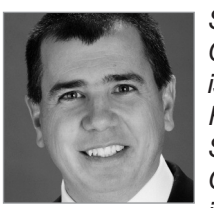
For all the other clients who aren't audited, no such formal requirements exist. Arguably these clients may possess the greatest risks, as there are no requirements for anyone internal or external to the organization to objectively review their controls and procedures. They may also pose the greatest risk to the accounting firm from a litigation perspective.

Several years ago while working for a regional firm we identified this very issue, and decided as a firm to take the proactive initiative to speak with all of our non-audit clients. Letters were sent to each client alerting them to the risks of employee theft and embezzlement, and internal newsletter articles were directed toward these issues. In some cases we met with the clients to discuss this and followed up with a letter summarizing our meeting. Many clients expressed their appreciation for educating them and causing them to change how they ran things. The goal was twofold: educate the non-audit clients and protect the firm as best as possible from potential future litigation.

Clients need to hear and understand that individuals in positions of "trust" are frequently the same individuals who embezzle large amounts of funds. "Trust" has no place within properly designed internal controls and procedures. Appropriate and practical controls should rely upon positions, levels of responsibility and areas of opportunity, and should not be subjectively based upon who currently fills a position.

Where do we go from here?

When evaluating internal controls, whether they are your own organization's or those of your clients, consider basic manual controls that were present in most accounting departments more than 20 years ago during the period before computers and the internet dominated most accounting areas. In many cases, easily identifiable basic level manual controls can minimize the risk of employee theft and embezzlement within any organization, but only if the controls are actually performed once implemented. And as always, remain vigilant.



Stephen Pedneault, CPA, CFE, CFF, FCPA is the principal of Forensic Accounting Services, LLC in Glastonbury, specializing only in forensic accounting, employee fraud, and litigation support matters. Pedneault is a Certified Fraud Examiner (CFE) and Certified in Financial Forensics (CFF). He can be reached via email at Steve@forensicaccountingservices.com. To find more information about Forensic Accounting Services, visit www.forensicaccountingservices.com.

Pedneault's new book Preventing and Detecting Employee Theft and Embezzlement: A Practical Guide *(Wiley) covers internal controls and procedures as well as all the financial areas typically found in most organizations, from hiring through month-end processing.*