Connecticut Law Tribune
FEBRUARY 22, 2010
VOL. 36, NO. 8 • $10.00
An ALM Publication
CTLAWTRIBUNE.COM

STAVING OFF CRIMINAL ACTIVITY

Internal controls cut down on employee thefts

By STEPHEN PEDNEAULT

The risk of employee theft has plagued employers for as long as businesses have had employees. Before the discovery of significant financial improprieties in 2001 with Enron and Worldcom, little attention was devoted to financial crimes including employee embezzlements.

Since 2001, it seems more instances of financial crimes and embezzlement have made news, raising the question whether the instances of fraud have been on the rise or the level of awareness simply is a result of the amount of attention these crimes now receive.

Statistically, one out of every nine financial crimes receives public attention. Coupled with the weak economy, growing unemployment rate, and historically high foreclosure rates, individuals in positions of trust may have the highest level of financial pressure in their personal lives.

Honest employees pushed to the limit to meet their financial needs and obligations are resorting to acts of desperation to avoid personal financial ruin without thoroughly thinking through the consequences if they are caught.

Law firms have not been immune from these crimes.

In several relatively recent cases, the amount of loss at the hands of law firm employees has been staggering.

Organizational Overview

In many of the cases, basic internal controls were not in place within the organization, or worse, the controls were not being followed. Complacency seems be a leading cause of financial loss.

I contend that fraud has not changed over the years, and that there is a finite number of ways employees can steal. Computers, handheld devices and paperless environments certainly add to the methods, but in the end how employees steal and in what area they divert funds remains the same.

Every business and organization has three basic accounting cycles: cash receipts; cash disbursements; and payroll.

Within each cycle there can be various types of transactions, and depending on whether the accounting is maintained on the cash basis or the accrual basis, there could be more or less of each type. A typical cash receipts cycle could include sales; sales returns; invoicing; cash receipts (cash, checks, credit cards and electronic payments to name a few); and unpaid accounts follow-up (accounts receivable). These transactions complete the life cycle of a sale.

The cash disbursement cycle would include purchasing; receiving; cash disbursements (paper checks and electronic payments); petty cash; credit card purchases; and unpaid vendor balance maintenance (accounts payable).

The payroll cycle would incorporate hiring, firing, and employee maintenance; time tracking; payroll entry; payroll processing; paycheck and direct deposit distribution; funding of payroll liabilities; and filing of payroll tax returns.

More complex organizations would also have additional accounting cycles, such as inventory, work-in-process, customer deposits, and fixed assets to name a few.


Stephen Pedneault

Lastly, transactions can cross accounting cycles, such as product sales that result in the recording of an invoice (accounts receivable), as well as the relieving of inventory (the product shipped to a customer).

Back To Basics

Every employer, regardless of size, needs to identify, implement and monitor a minimal level of internal controls.

Simply delegating tasks and responsibilities to "trusted" individuals is a recipe for financial disaster. Even in the smallest of businesses with one employee, the risk remains, and basic controls need to be identified and enforced. These same basic controls found in the smallest organizations would likely prevent or detect many of the largest embezzlements capturing the headlines.

Just what are some basic level internal controls?

The following is a list of basic controls every business should consider implementing. The list is not intended to provide absolute assurance that employee theft and embezzlement cannot occur. Quite the contrary, individuals under pressure will work hard to find ways around these controls or some other way beyond these controls. Therefore, it is incumbent upon every employer to remain vigilant, and to constantly review the

Stephen Pedneault is the principal of Forensic Accounting Services LLC in Glastonbury, specializing only in forensic accounting, employee fraud and litigation support matters. He is a Certified Fraud Examiner and Certified in Financial Forensics and author of three books on fraud and financial crimes.

Forensic accounting & valuation litigation

accounting and bookkeeping areas to ensure no individuals have found ways to divert funds away from the organization.

Cash Receipts

- Any new customers or clients must be independently reviewed and approved before being added to the system and granted credit status.
- Payments received must be reconciled to payments posted to the system and also to the bank deposits on a daily basis (three-way reconciliations).
- If possible, individuals handling payments should be independent of individuals with access to post payments and adjustments to customer accounts.
- Any non-payment adjustments need to be documented, approved and reviewed regularly so diverted payments are not concealed through adjustments.

Cash Disbursements

- An original vendor invoice or receipt is required to support every disbursement.
- Every disbursement should be made by computer-generated check (no manual checks) or by electronic payment.
- Supporting original invoices and receipts must accompany every check for the signer's review and approval.
- Checks are to be manually signed (no signature stamps), and a second signature should be considered for checks over a stated dollar amount.
- All electronic payments are to be processed by authorized bank signers only, consistent with paper check signing.
- The bank statements along with cancelled check images are to be received directly by the primary signer unopened (ideally at their residence) to be reviewed for reasonableness and returned for timely bank reconciliations.
- The completed bank reconciliations for every bank account are to be reviewed for reasonableness and approved.

Payroll

- Every new employee, or change to any existing employee, should be documented and approved prior to making changes within payroll.
- Ideally, the individual responsible for employee maintenance should be different from the individual who processes payroll.
- All time and attendance information, hours and earnings must be reviewed and approved prior to processing the final payroll for each payroll cycle.
- The payroll registers, reports and other supporting information are to be received directly and unopened by an owner or appropriate designee.
- The payroll registers and reports are to be reviewed for reasonableness and approved for each and every payroll cycle.
- If a CD-ROM containing images of the payroll reports is received, the payroll registers and other appropriate reports are to be reviewed (on screen or printed) for each and every payroll cycle.

Bank Activity

It is incumbent to monitor the activity of each and every bank account on a regular if not daily basis. Financial crimes committed against bank accounts by outsiders are staggering, and financial institutions have begun pushing the fraud expenses back to their customers.

Three of my banks now follow a policy whereby I have five business days to identify potentially fraudulent activity within my bank account and notify my bank. In the event I do notify them timely, not much has changed. However, if the bank can show that I should have identified the activity within five days and didn't notify the bank, then my exposure is $500.

I suspect the levels of loss the customer will bear will increase as well. ■