Connecticut Law Tribune
FEBRUARY 23, 2009
VOL. 35, NO. 8 • $10.00
An incisivemedia publication
CTLAWTRIBUNE.COM

Guarding Against Employee Theft And Embezzlement

Three-step approach to protecting your firm and client funds

By STEPHEN PEDNEAULT

Employee fraud and embezzlement have the greatest impact on the partners of law practices, especially smaller firms. Beyond the loss of funds often requiring partners to contribute personally to make client accounts whole, thefts involving client funds often result in the firm answering to the Statewide Grievance Committee.

The number of embezzlements within Connecticut law firms in just the last two years has been staggering, as has been the amount of funds involved. Taking into account the current declining state of the economy, it is safe to say there are employees stealing (or should I say "borrowing") as I write this article. The questions are how do you identify who is stealing, how long they have been stealing, how much they have taken, and whether client related funds or the firm's IOLTA accounts are involved in the scheme.

Risk Assessment

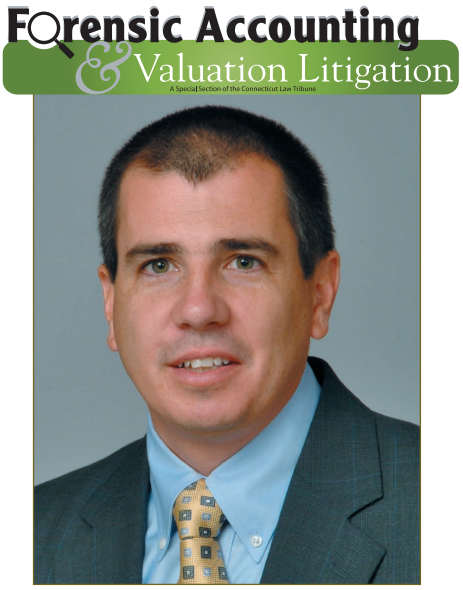
A good place to start is to identify all the financial areas within the firm where employees have access to funds, any funds, also known as "opportunity." Beyond the firm's operating cycles, which include billing and collections, cash disbursements and payroll, many practices administer client estates and trusts, manage client funds, facilitate real estate closings through client fund accounts and act as escrow agents for client matters. Firm employees often perform the bookkeeping and accounting functions, creating opportunities for employee theft in these areas.

No financial areas are free from risk for employee theft. For example, embezzling employees have long determined that client checks made payable to the firm can be diverted and converted for personal use by simply depositing the stolen checks into their personal bank accounts via an ATM machine.

Another scheme that has been surfacing involves funding instructions for real estate closings. With a simple change to funding instructions, the closing proceeds can be forwarded to an employee's personal bank account. As long as the perpetrator is the same person who reconciles the closing account and a sufficient volume of closings continue, the "float" in the account should cover the theft (for a while).

Employee theft involving client trust accounts is amongst my top three schemes investigated in recent years. Employees responsible for trust activity and maintaining the bookkeeping use client trust funds for personal use. Often there is no segregation of duties and the same individuals conceal their thefts within the accountings and reconciliations they provide.

Similar thefts have surfaced at an increasing rate involving client fund and IOLTA



accounts. Firms often rely on the same employees to facilitate transactions, record activity and reconcile these accounts. Funds are diverted and concealed by the employee. All too frequently the theft goes undetected and is only identified after a check is returned by the bank for insufficient funds in an account that should never have insufficient funds, triggering an automatic referral to a grievance committee.

What Can You Do?

A three-step approach is recommended for any organization with employees. The three steps form the corners of the fraud risk triangle.

Preventive Controls

Safeguarding measures, also known as

Stephen Pedneault is a CPA, certified fraud examiner, certified in financial forensics and a forensic certified public accountant. He is the principal and founder of Forensic Accounting Services LLC in Glastonbury, specializing in financial investigations to uncover fraud and embezzlement. His book, "Fraud 101," published by Wiley Press, will be available late Spring 2009. For more information, visit www.forensicaccountingservices.com

internal controls, need to be implemented by every firm, regardless of size, within each identified financial area to prevent thefts from occurring. Limiting check-signing to partners, requiring supporting invoices and documentation to accompany every check to be signed, and hand-signing (versus signature stamps) all checks are great controls to implement.

Bank lock box services can ensure all firm payments received are properly deposited every day, providing same-day availability to funds and removing access to client payments from employees. Employees receive and record payments from copies provided by the bank. Bank desktop depositing could also allow partners to receive the mail, complete the daily deposits without leaving their desk, and then provide the payments to employees for posting, ensuring all payments received are properly deposited.

Most payroll systems allow for pre-payroll reports prior to actually processing payroll. An independent review of the pre-payroll report could identify a potential issue prior to processing. The same report could also be compared to the actual payroll reports once received from the payroll provider to ensure no changes were made.

Detection Measures

Proactive preventive controls will not provide adequate protection against many employee fraud schemes. The second line of defense to minimize the firm's loss and exposure involves the firm implementing detection measures for each identified financial risk area. The goal is to detect employee thefts as early as possible.

First and foremost, every bank statement should be mailed directly to a partner, ideally the partner who is the primary check signer on the account. The bank statement should be received unopened. The partner should review the statement and check images (if received) for reasonableness. This applies to every type of account. Many employee frauds should be identified in the first month using this measure.

The firm's payroll should be handled in a similar fashion – received by a partner from the payroll vendor, reviewed for reasonableness and then forwarded for processing and distribution.

If the firm accepts credit card payments from clients, use the same process again for the monthly merchant statement. Look for credits processed to employee cards, reducing their outstanding balance on their account.

Account reconciliations need to be performed monthly in a complete, accurate and timely fashion for every bank account. Ideally, reconciliations should be performed by someone other than the employee whose primarily responsibilities involve the account activity. Completed bank reconciliations need to be reviewed by a partner.

This is especially important for all client funds and IOLTA accounts in light of the random audits being performed by the auditors for the grievance committee.

Daily reconciliations should be implemented over client payments to ensure all payments received are reconciled to the deposit and also to the payments posted to the firm's accounts receivable system.

The best way to approach what measures to implement is to look at each financial area in the firm and identify how employee thefts could occur within each area. Next, identify practical measures that can be implemented to detect potential issues. Random reviews of activity and account reconciliations provide both a deterrent effect, as well as, a measure for detection.

Employee Dishonesty Insurance

Insurance coverage typically allows a firm to recover a loss resulting from an employee theft. Even with expertly designed preventive controls and detection measures in place, employee theft and embezzlement remains a risk. Dishonest people seem to have an unlimited capacity for creativity when it comes to "beating the system." Often, when a substantial amount of money is stolen and identified late in the scheme, the funds are unrecoverable except through an insurance policy.

Firms should estimate the minimum amount of insurance coverage needed to ensure the financial health of the practice, keeping in mind that $100,000 is usually the recommended minimum for any size firm. Coverage typically covers losses only after the date of insurance.

Talk To Your Clients

There is no industry or any size or type of organization immune from this threat. When combined with outsider fraud, such as counterfeit checks and vendor kickbacks, losses attributable to fraud and abuse can exceed 8 percent of annual revenues.

Virtually every business collects payments, processes credit cards, writes checks and pays employees. Those four areas compose a vast source of opportunity for employees to divert funds from their employers. While it may not be feasible to eliminate risk in any one of these areas, employers can institute several critical controls to minimize their risk.

The lesson for every employer when it comes to employee fraud and embezzlement is to avoid complacency. Maintain constant vigilance and never simply trust that employees are trustworthy and ethical. To quote the late Ronald Reagan, "trust with verification" is the best policy. ■