SIGNS OF FRAUD: A CASE BY CASE REVIEW

*By **Neil H. Fishman***

ALL COMPANIES NEED TO APPEAR VIGILANT to deter employees that might consider breaking the law.

Fraud can create problems for any company; it can occur in almost any facet of a business and can be committed by any number of individuals. Despite a company's size or internal safeguards, there is no getting around one simple fact: Dishonest individuals are everywhere. Motivated by the belief that they cannot or will not be caught, dishonest employees can find ways to circumvent a company's policies and procedures. All companies need to be mindful of fraud and at least appear vigilant to deter employees that might consider breaking the law.

Payroll

Manipulating a company's payroll is one of the most common forms of fraud, and there are many ways to make it happen. One way is to hire "ghost employees," fictitious or real individuals that receive a paycheck but do not work for the company. A ghost employee might be a relative or friend of the perpetrator. For this scheme to work, the person who hires new employees must be either an active participant or an unsuspecting victim.

Case No. 1: A supervisor added several ghost employees to his maintenance payroll. The individuals actually existed, but they worked for other companies. The supervisor filled out fake timecards, and when the "employees" received their checks, they cashed them and split the proceeds with the supervisor. The supervisor was able to commit this fraud because he had the authority to hire and supervise employees.

Another type of payroll fraud occurs when an employee in a personnel or payroll department adds "new" employees.

Case No. 2: A payroll department employee had the authority to enter new employees, correct information, and distribute checks. The department supervisor trusted the employee to perform the work and did not independently verify it. This absence of review, combined with the lack of separation of duties, made it very easy to add "new" employees into the company records.

Ex-employees can unknowingly facilitate a ghost employee scheme: Checks are still generated for these individuals, but the perpetrator then intercepts them.

Companies that use manually prepared timecards can fall victim to a falsified hours and salary scheme. To falsify the number of hours worked, the supervisor's signature might be forged, the supervisor might conspire with the employee, or the supervisor might fail to review timecards for accuracy before submitting them for processing.

Case No. 3: Employees wanted better work areas and assignments. The supervisor was more than willing to accommodate them—for a price. Timecards were falsified, then approved by the supervisor. Employees received payment for additional overtime, which was kicked back to the supervisor.

Case No. 4: After noticing that the manager did not reconcile the hours approved on time cards to the hours paid in the expense journal on a regular basis, an employee created fictitious time reports, resulting in more than $30,000 in fraudulent wages. Since the expense journal was not reviewed, this simple scheme went on for some time before being detected.

Timecard schemes are not the only way to generate fraudulent wages: In certain instances, salaried employees have tried to generate false wages by manipulating incentive program elements. Employees, sales representatives, and brokers that draw a salary based on or augmented by a percentage of their sales have been known to commit payroll fraud through a commission scheme. The perpetrator creates fictitious sales by tampering with sales orders, purchase orders, credit authorizations, packing slips, and other documentation or through the less sophisticated method of ringing them up on a cash register.

Case No. 5: In a recent high-profile case, an employee at a major brokerage house in New York City received a seven-figure bonus for the sale of municipal bonds. It was later determined that these sales were fraudulent, and the employee had to return the bonus.

Case No. 6: A salesperson in a clothing store rang up sales to an accomplice. After splitting the commission check, the perpetrators returned the purchased items.

Accounts Receivable

Accounts receivable is also susceptible to fraud, generally involving the simultaneous manipulation of sales and inventory. Depending on the work responsibilities of the individuals involved, schemes affecting accounts receivable deal with fictitious receivables, cash skimming, larceny, failure to write off receivables upon receipt of payment, and improperly writing down receivables as bad debts.

Case No. 7: Payments are posted to the accounts receivable ledger, but the money is taken by the employee. The employee had control over the company's deposits and ledgers and was able to make unsubstantiated journal entries to balance the books and records fictitiously.

Case No. 8: By failing to itemize the daily receipts, there was no way to pinpoint which customers had paid which amounts. This enabled the employee in charge of recording the receipts to skim a portion of the payments, which over a period of time totaled more than $10,000.

In many cases, especially in small businesses where there are few employees to share responsibilities, manipulating records is easy. Cash receipts are vulnerable because they can be recorded in the accounts receivable journal and pocketed.

Case No. 9: The office manager handled the books of a medical practice, and there was no one to check on what was done. On several occasions patients paid by cash or check on outstanding balances. In each instance, the office manager recorded that the money was received against the balance but pocketed the money instead of depositing it in the business account.

Employees can also understate sales by failing to report them or by writing them down as less than their actual worth.

Editor:
Robert H. Colson, PhD, CPA
The CPA Journal

Case No. 10: An employee wrote up receipts for sales but removed the carbon paper so that the company copy was not made. The employee then wrote the company copy in pencil, reported a $100 sale as $80, and pocketed the $20 difference.

Case No. 11: A store manager opened for business at 8 a.m. while normal business hours started at 10 a.m. For two hours business was conducted and sales were made but not recorded. Just as sales can be understated, inventory can be manipulated through fraudulent returns.

Case No. 12: A cashier recorded a returned item as a different, higher priced item. The customer received a full refund for the purchased item, and the cashier pocketed the difference.

Accounts Payable

Another common form of fraud involves accounts payable, which might include the fraudulent purchase of supplies and materials and other general expenses. Accounts payable can be manipulated in several ways, and paying attention to the purchaser is as important as keeping an eye on the actual purchase.

Case No. 13: A purchasing agent had a very good relationship with some of a company's suppliers. On a surprise check on bids for a new project, it was discovered that the supplier chosen was charging a per unit price higher than other submitted bids. It turned out that this supplier was giving the purchasing agent a "commission" for each winning bid. Further investigation revealed that this supplier was chosen frequently in the past, despite bidding higher than other vendors.

Altering checks is another means of defrauding accounts payable. Similarly, so is the shell company scheme.

Case No. 14: The bookkeeper typed out the checks to the suppliers, which were then signed by the company owner. The bookkeeper used an erasing typewriter to remove the payee designation and amount from the check and replace them with her name and a significantly greater amount. These amounts were entered in the disbursements journal as payments for aggregate inventory to the company's largest supplier, who received several large checks each month. More than $300,000 was stolen in this manner.

Case No. 15: A department head set up a dummy corporation and used his home address as the mailing address. Over a two-year period, the department head submitted false invoices for more than $250,000. This scheme was eventually detected when a new employee noticed that the vendor's address matched her boss's address. If a P.O. box had been used, this scheme might have continued indefinitely. ❑

Neil H. Fishman, CFE, CPA, *is a principal in Fishman Associates CPAs PC. He can be reached at fishcpa@ix.netcom.com.*

A number of cases cited in the article are derived from Occupational Fraud and Abuse, *by Joseph T. Wells (Obsidian, 1997).*