

**\$600
BILLION
IS LOST TO EMPLOYEE
FRAUD
ANNUALLY**

*Six simple procedures to help
minimize your risk of employee fraud.*

AHLBECK & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

STOP FRAUD BEFORE IT BECOMES A PROBLEM

Should you be concerned about fraud? Absolutely! Approximately \$4,500 per employee is lost annually as a result of fraud, according to the Association of Certified Fraud Examiners. Small businesses are the most vulnerable, resulting in average losses of \$127,500 per scheme. Consider the following:

- 39% of frauds occur in companies of less than 100 employees
- Most fraud schemes last longer than 12 months before being detected
- Typical fraudsters are long-time employees committing their first offense

THREE FACTORS EXIST IN THE MAJORITY OF FRAUDS:

- **Pressure** - A financial need causes someone so much stress that they turn to fraud
- **Rationalization** - Coming to terms with the fraud by feeling entitled to it or the belief that everyone else is doing it
- **Perceived Opportunity** - Operations may provide the opportunity to commit the fraud with little chance of being caught

Limiting perceived opportunity can greatly reduce the risk of fraud. Our six simple procedures can help minimize your risk of employee fraud and increase your awareness of the everyday risk involved.

AHLBECK & COMPANY

Certified Public Accountants and Business Advisors

Ahlbeck & Company is a certified public accounting firm providing accounting, auditing, tax and related business advisory services. With a strong emphasis on client commitment, the firm has continued to grow over the past 40 years, serving individuals, businesses and not-for-profit organizations.

The professionals at Ahlbeck & Company take pride in their work to deliver above your expectations, earning the trust and respect of clients through exceptional service.



EVALUATE YOUR SYSTEM

Although some fraud risks are inherent, most can be addressed with an appropriate internal control system which includes the following:

- a well-developed control environment
- a secure information system
- proper monitoring activities

Modification may be required for areas identified as having a higher risk of fraudulent activity, as well as controls over the company's financial reporting process. **Ongoing evaluation, monitoring and modification of current systems** is one of the most significant ways to minimize fraud.

In evaluating internal control systems, smaller businesses often have difficulty segregating duties and responsibilities due to size. *At a minimum*, however, the following should be adhered to:

- No single individual should maintain the accounting records, collect monies, write checks and reconcile bank accounts. Allowing one employee this responsibility is an organizational flaw that leaves the company vulnerable. It provides a perceived opportunity to commit fraud with little or no chance of being caught.

Ineffective or absent controls can create situations in which an employee may “doctor” a bank reconciliation or create fraudulent accounting records to conceal misappropriated funds. Statistics show that typical fraudsters are long-time employees with no prior offense, so relying on an employee's clean track record and longevity with the company should not be considered a control or deterrent in and of itself.

DID YOU KNOW...

In approximately 86% of fraud cases, victims had either insufficient internal controls or allowed their controls to be ignored by employees and/or management, according to a study by certified fraud examiners. A strong system of internal controls is one of the most effective anti-fraud measures.

- The bank statement should be delivered to the owner, executive director, treasurer, or other person independent of routine accounting activities. Additional oversight from “outside” the system strengthens the internal control system by providing a stronger independence factor.

Assigning a higher-level employee this responsibility adds an additional level to the review function, thereby reducing an employee's ability to perpetrate an undetected fraud.

2 SECURE CASH

Statistics show that cash is targeted 90% of the time in fraud schemes. Two types of cash receipts fraud include *skimming*, in which cash is stolen before it is recorded on the company's books, and *cash larceny*, whereby cash is stolen after being recorded by the company.

DID YOU KNOW...

The majority of asset misappropriation involves theft of cash due to its defined value and ease of movement and conversion. Although less common, schemes involving non-cash assets, such as inventory or equipment, were more costly, averaging \$200,000 per scheme.

One of the most important ways to prevent cash fraud is to **keep cash in a secured manner** prior to making the bank deposit. This can include a lockbox, safe or other protected location.

In addition, access should be restricted to only those employees with proper authorization who need to access cash funds as part of their job responsibility. Receipt of cash should be as centralized as possible.

Businesses that receive a large volume of checks through the mail often use a lockbox system to strengthen internal control and facilitate the immediate deposit of cash receipts from a central location.

Companies such as retail businesses or restaurants are also susceptible to theft of cash on hand if they handle large amounts of cash. This can be perpetrated through fictitious refunds, altered credit card receipts and "skimming" cash (accepting cash but not preparing a receipt).

Theft of cash on hand is normally not material to a company's financial statements; however, management should be alert to the possibility.

3 SEPARATE BANKING RESPONSIBILITIES

One area especially susceptible to fraud involves banking. This includes deposits as well as reconciliation. Overall, cash receipts are involved in 40% of cash frauds, averaging \$60,000 per cash receipts fraud scheme! How can you protect your company from this type of fraud?

Ideally, one of the strongest controls is **segregation of duties for making bank deposits, deposit reconciliation and bank statement reconciliation.**

Bank deposits should be made daily by an employee without responsibility for opening the mail or managing accounts receivable. This eliminates the opportunity to “skim” cash received in the mail and alter the bank deposit slip or customer records to conceal the fraud.

Bank deposits should also be independently reconciled and verified to funds received in the daily mail.

Bank reconciliations should be prepared on a timely basis by an employee not responsible for the issuance of checks or custody of cash.

In addition, the reconciliations should be reviewed by a higher level in management, noting any large, unusual or recurring reconciling items.

DID YOU KNOW...

Smaller companies (100 or less employees) experience higher median fraud losses than companies with 10,000 employees or more. Lack of proper accounting controls, including segregation of duties, is one key factor. An increased level of trust between co-workers can also cause employees to be less alert to the potential for dishonesty.

You can also keep your system controls effective and reduce the risk of fraud through:

- unannounced cash counts
- observation of cash handling
- independent review of reconciliations

4

REVIEW PAYROLL

Are you aware that the average payroll fraud involves \$140,000 per scheme, with 39% of frauds occurring in companies of less than 100 employees?

Payroll fraud can involve “ghost” employees, falsified hours and salary, and commission overstatement. There are, however, procedures that can minimize your risk.

DID YOU KNOW...

Employees who feel well-treated and adequately compensated are less likely to commit fraud than those who hold grudges against their employers – whether justified or not. Employee attitude in the workplace can affect whether or not fraud is committed.

The most common payroll fraud is the use of “ghost” employees, whereby the fraudster enters fictitious employees into the payroll system and receives the resulting payroll checks. A variation of this scheme includes employees on the payroll with duplicate addresses or social security numbers, or no withholding amounts or other normal payroll deductions.

Ideally, personnel files should be maintained independently of time-keeping and payroll disbursement to allow for segregation of duties in your internal control system.

One procedure that can minimize your company’s risk is to **independently review payroll disbursement registers, paychecks and annual W-2s** before they are distributed. This allows for any irregularities to be analyzed and addressed on a timely basis.

Appropriate approval should also be required for time worked, rate of pay, bonuses and overtime. This same approval process should be applied to commissions as well.

Procedures to effectively check up on your systems and ensure controls are operating effectively include:

- spot-checking independent approval of hours worked and pay rate
- comparing paychecks to an employee list

5 CONTROL YOUR CHECK SYSTEM

What is check fraud? Schemes vary but include forging, altering and stealing checks, with the average check tampering fraud involving \$140,000 per scheme!

One of the most important procedures in your internal control system concerns **support for disbursements by check**. When a check is submitted for signing, it should be accompanied by *original* documentation supporting the disbursement. Copies of support should not be accepted as they can easily be altered.

If no invoice exists (for example, in the case of expense reimbursement), a voucher explaining the expense should be signed by the requester.

Once signed, checks should remain in the control of the authorized signer until mailed. Checks should not be returned to the custody of the employee who prepared them for signature as tampering or alteration could occur at this point in the process.

Management can monitor check system procedures by:

- performing a detailed comparison between cancelled checks and the disbursements journal
- investigating reconciling items on the bank reconciliation to check for irregularities or discrepancies

One of the most common sense procedures is to report lost or stolen checks *immediately*. Don't wait, thinking they were just misplaced. A delay of just 24 hours can cost your company thousands of dollars!

DID YOU KNOW...

Statistics show that 71% of cash frauds involve fraudulent disbursements, in which the perpetrator uses company checks to either withdraw cash directly for their own benefit or pay personal expenses.

6 KNOW YOUR VENDORS

For many small businesses, billing represents the largest risk of embezzlement, with most billing fraud schemes lasting more than 23 months before being detected.

The most common billing fraud scheme is the payment of invoices to a fictitious company. The fraudster establishes a fake identity (often using a name similar to that of a legitimate vendor) and gets that information entered into the company records as a genuine vendor.

Several procedures can be followed to avoid these types of fraud. An *approved* vendor list should be maintained by an independent person and compared to payees to ensure there are no deviations.

Procedures should be established to ensure that major purchases are bid competitively. This includes proper review and approval of bids by management to ensure a fair and objective process.

Invoices should be approved before payment and marked as such on the *original* invoice to eliminate the risk of duplicate payment.

DID YOU KNOW...

Collusion between employees and managers can be difficult to prevent and detect because managers often have a key role in the company's internal control structure. Fraud statistics indicate that schemes involving collusion between employees and managers resulted in median losses of \$500,000 per scheme, eight times greater than losses incurred through schemes in which the employees acted alone.

Billing fraud schemes often require collusion. Separation of purchasing, invoice approval, receiving and payment responsibilities are strong internal controls that reduce the risk of billing fraud from collusion.

The effectiveness of your internal control system can be increased by:

- comparison of budgeted expenses to actual
- appropriate management oversight through questioning purchases and billings

AHLBECK & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

1665 Elk Boulevard • Des Plaines, IL 60016

Tel: 847/824-4000 • Fax: 847/824-4012 • www.ahlbeckco.com