

Fraud 101: Small business at risk

FRAUD: 1. Intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right 2. The act of deceiving or misrepresenting. That's how Webster's Dictionary defines the word "fraud"

Business fraud and abuse costs have reached \$400 BILLION dollars a year. That equates to \$9.00 per employee, per day. Pretty incredible isn't it! It appears that the work force today has become Ethically Challenged. Who's the most at risk? The answer, small businesses.

Fraud is difficult and often impossible to prevent.

However, if after reading this, you open your eyes a little wider, look a little closer, and pay stricter attention, you may not become part of these startling statistics.

The goal of a fraud prevention program should be to implement procedures and establish systems that provide obstacles to those who attempt to commit fraud.

Below are some of the different fraud schemes, most you have heard of, maybe a few you have not.

- Embezzlement
- Forgery
- Phantom Vendors/Purchasing Fraud
- Kickbacks/Secret Commissions
- Travel & Expense Account Fraud
- Inventory Theft
- Payroll Fraud
- Billing Fraud
- Kickbacks/Vendor Fraud
- Check Fraud/Forgery
- Theft of Company Secrets

Following are some fraud "red flags" you should look for:

- A prior history of fraud occurring in the company.
- Loose internal controls within the company.
- No corporate compliance or ethics program in place.
- Noticeable personality changes in employees.
- Employees living beyond their means (cars, vacations, wardrobe).
- The employee(s) who never, or rarely, take(s) a vacation.
- An unexpected or unexplainable drop in earnings.
- Complaints of errors or shortages from customers and/or employees.
- Missing documents and sloppy bookkeeping.
- Accounts that are out of balance.
- A concentration of authority in a few individuals (lack of

separation of duties).

- The absence of original invoices, with copies substituted instead.
- Unexplained inventory shortages.
- Unauthorized access to computer files and proprietary information databases.

Once you have established what type of fraud risks exist in your company, you will want to develop an innovative and effective anti-fraud program. Some ideas you may want to include are listed below.

- A proactive ethics program or manual.
- Establish penalties and prosecution policies.
- Make sure your company's standards, procedures and penalties are effectively communicated to employees at all levels. A 'no tolerance' approach.
- Develop an anti-fraud partnership with vendors and business associates.
- Pre-employment screening.
- Employee exit interviews.
- Set up funds transfers electronically for payroll and other recurring forms of disbursements.
- Training should stress that not all assets are physical.
- Your company should have clear policies on prohibiting conflicts of interest.

Once your company's policies and procedures have been established you will want to periodically review, evaluate and test your anti-fraud program. You may also want to have legal counsel review the program which will be enforced by security and possibly used as grounds for dismissal should any violation occur.

White collar crime is simply a fact of corporate and institutional life. Because there are so many types of fraud, companies have to be ever vigilant. But strong policies, consistent enforcement, and well-thought-out awareness training can stop most would-be schemers from making the company an easy mark.

info@fraudiscovery.com
16255 Ventura Boulevard, Suite 525
Encino, CA 91436-2310 USA
(800) 856-9948

AccountingWEB.com May-12-2008