

PROTECT YOUR COMPANY



## Top 20 Ways to Reduce Your Company's Fraud Risk



FORENSIC ACCOUNTING  
& INVESTIGATIVE SERVICES

## **1 | Sign up for a Fraud Hotline Service**

Fraud hotlines offer an anonymous way for people connected with your business to report suspicious activity. The majority of frauds are uncovered through hotline tips. Keep your fraud hotline number visible, as many frauds are called into hotlines by employees and vendors. Fraud hotlines prove invaluable by acting as an additional security feature protecting the integrity of your business.

Eide Bailly offers a free fraud hotline answered by trained fraud investigators, on call 24/7. There is a \$75 charge for someone to take a report, and you must sign up for the service beforehand. The follow-up investigation on a tip is a separate engagement. **To sign up, call 1.866.999.8362 or visit our website: [http://www.eidebailly.com/services/forensic/ol\\_hotline/fhotline\\_engagement\\_form.aspx](http://www.eidebailly.com/services/forensic/ol_hotline/fhotline_engagement_form.aspx)**

## **2 | Require a Background Check on all Employees**

Background reports are inexpensive and a great way to protect the culture and quality of your business.

- Check for inconsistencies between the application and the background report. A person's dishonesty can prove detrimental to your business. When dishonesty is apparent, you should look deeper into the candidate's background or consider another candidate.
- Be especially diligent about checking backgrounds on employees who enter people's homes. Failing to utilize background checks could create additional liability for the company.
- Know who you are hiring. Use their application. Take time to call previous employers and listed references. If you take a few minutes to make phone call, you may find out more than you expected.

## **3 | Be Actively Involved in Your Company's Finances**

Check your company's bank balance and expenditures on a monthly basis. Know what it costs to run your company. Be able to recognize when expenses seem too high, or revenue seems too low for the company's volume of sales.

- Send your payables and receivables to a P.O. Box, not your office.
- Open and read your mail. Know how much money is coming in and going out, then bring it to your bookkeeper. If you can, segregate the duties. Have your receptionist or office manager open, list and log all checks received in the mail. Then review reconciled bank statements and compare the check log to the deposit slips.

## **4 | Review Your Company's Financials**

Fully review your company's financial statements. Read beyond the first page of the Profit and Loss Statements—review every item on every page. A fraudulent employee will try to hide the fraud loss in detail level pages; if you don't examine your company's statements thoroughly, these red flags will be impossible to find.

- Don't manage by the bottom line. You cannot know exactly how your company is doing by simply looking at your bottom line
- If you don't understand something on your P&L, ask questions until you do. It can help to rename things you don't understand so that they make sense to you.
- Know what each line item on your financial statement is. It's your company. It is vital that you understand how every piece is put together.

## **5 | Check Books Regularly and Without Warning**

Be watchful for things like reoccurring charges, employees you don't know you hired, expenses you don't remember signing for, excessive voids and duplicate payments.

## **6 | Sign Your Own Checks**

Avoid stamp signatures whenever possible.

## **7 | Limit Access to Key Data**

Each employee should have his or her own passwords and controls. All financial programs should have ways to limit access to valuable information.

## **8 | Incorporate Passwords and User IDs**

Each employee should have their own password and user ID to sign into their computer. Also, implement an automatic sign off when the computer is not being used.

## **9 | Safeguard Passwords**

Keep passwords secret, not posted on the computer via a sticky note. Make sure sensitive company, employee and customer information doesn't make its way into the wrong hands.

**10 | Establish Policies for Credit Purchases**  
Have employees sign contracts indicating that they will not make any personal purchases on the card, and that they are responsible for any personal charges. Company policy should state that misuse will result in termination.

- Have restrictions to the account assigned by the bank based on spending limits or merchant accounting codes. This will ensure employees can only spend up to approved amounts at approved locations.
- Establish specific rules for company credit card use.
- Be extremely careful when initially giving out the privilege to use the company credit card. Once the privilege has been extended, the police cannot always prosecute the employee if the card is used differently than the owner intended.

**11 | Checks and Balances**  
Implement a “checks and balances” program at your company, for everyone—even you.

There are many companies where employees’ work goes unchecked. This allows employees to commit fraud more easily, because they know no one is watching. Operating without a system of checks and balances can end up costing the company significantly, even leading to bankruptcy.

When internal controls are established and everyone knows their work will be double-checked, the opportunity for fraud is greatly reduced. The bottom line: using checks and balances makes trusting your employees easier.

**12 | Get a Fraud Assessment**  
Eide Bailly can assess your business and identify any weaknesses in your controls, as well as areas where people could potentially steal from you. We talk with employees in your business on every level to establish controls with checks and balances. This initial assessment also sets a foundation for future assessments, so that you can quickly and affordably continue to evolve your fraud protection to suit your changing business.

**13 | Implement Internal Controls**  
Ask the following questions to evaluate your current internal controls policies:

- Are blank checks left out?
- Do people have access to your signature stamps?
- Are you getting all the money owed to you? If you receive many checks in the mail, do you know how many actually come in your front door?

**14 | Learn About Computer Security**  
Most security breaches originate from within your company—usually from your employees or contractors. As an organization, you’re only as secure as your weakest point. In many companies, that means your internal network. Check your firewalls on a regular basis and have policies covering what is appropriate on company computers and what is not. Conduct random checks of your network, including your network staff, and make sure your IT policies are updated on a regular basis.

**15 | Increase the Perception of Getting Caught**  
• Perception of detection is one of the most effective deterrents to fraud. People rarely commit fraud if they think they will get caught.

- Make your office a fraud unfriendly place through fraud education programs with company personnel, fraud assessments, mandatory vacations, surveillance, fraud hotlines and violation enforcement.
- Commit to keeping your fraud program current. Some fraudsters will learn how to override your controls. A commitment to a responsive program keeps this in check.

**16 | Educate Your Employees About Fraud**  
Educating your employees helps raise awareness about fraud, including its impact on the company, and minimizing the opportunities available to fraudsters.

Here are three ways to empower your employees and help you fight fraud:

- Have fraud awareness training for your company. A brief, 45-minute talk twice a year helps employees recognize the subtle and not so subtle instances of fraud. Regular updates keep things fresh, and get new staff up to speed.
- Keep fraud awareness at the forefront. Management’s commitment to fraud education and re-education is the key to reducing your fraud risk. If management is committed and demonstrates that the organization is serious about their fraud program, their employees will follow.
- Implement a Fraud Hotline. (Refer to Strategy #1)

## **17| Institute a Code of Conduct and Fraud Policy**

- Set clear boundaries of what is and is not tolerated in your company. State the repercussions of the employees' dishonest actions. Employees must know the rules of the company in order to prevent breaking them.
- Be consistent in enforcing your code of conduct. The moment management diverts from the policy is the moment employees stop following it.

## **18| Obtain Employee Dishonesty Insurance**

Check to see if your company has employee dishonesty insurance. Most business insurance policies have small coverage allowance for employee dishonesty. Some insurance policies require prosecution or an accurate accounting of the loss to submit a claim. Forensic accountants at Eide Bailly can help you document your claim. Know what is required by your policy and the level of coverage you have.

## **19| Keep Your Professional Life Professional**

Affairs complicate things and add stress to the work environment. If a supervisor is having an affair with an employee and gives that person a bonus, there's no proof that he or she didn't authorize fraudulent bonuses based on historical proof to the contrary.

## **20| Be Observant**

Does someone appear to be living beyond his or her means? Is an employee going through a divorce or child custody dispute? Are they having an affair? Affairs are extremely costly (hotel rooms, flowers, dinners, etc.) and for the parties involved, using a personal credit card is often not an option. Therefore, individuals will use the company credit card so the charges aren't visible to their spouses. Also, the disposable income needed to carry on an affair has to come from somewhere. People will steal the money to continue the affair.

### **For More Information**

Call today—866.999.8362

[www.eidebailly.com](http://www.eidebailly.com)