



Ross, Pope & Company LLP

Chartered Accountants

Fraud - Protect Your Business!

Some suggestions for measures to "fraud proof" your business

In our practice, unfortunately we sometimes find successful business owners who have been taken advantage of by dishonest employees. Often the most significant losses stem from the hands of the most trusted employee who has full or partial custody of financial accounts and records.

One of the ways to prevent employee fraud is for the business owner to create a working culture that values honesty and integrity. When owners have a lax approach to company policies and procedures, staff may be more likely to "bend the rules", creating an opening for fraud. But when owners model an attitude of compliance to policies and procedures, employees will notice and follow.

Fraud proof your business by hiring competent individuals who have good records. Where possible, check the credit worthiness of potential employees, do a civil and criminal background check and certainly contact former employers.

Unfortunately, even trusted and honest employees can sometimes turn bad; this is why it is important for every business to implement and maintain a system of checks and balances that segregates key responsibilities. Ideally these checks and balances should be designed to make sure that the same employee does not authorize, process, and record financial transactions.

Most susceptible to fraud as a result of the lack of segregation of duties are cash receipts and disbursements. Below we have identified some tips to prevent such frauds.

- Enforce mandatory vacations for all accounting staff.
- Ensure bank statements with cleared cheques are mailed directly to the owner or to a trusted employee who is not responsible for recording financial transactions.
- Bank statements should be reviewed by a person not involved with bank reconciliations for alterations, appropriate endorsements and unauthorized payments, before they are given to the person preparing the bank reconciliation.
- Key analysis and ratios should be done by the owner every month.
- A person independent from the preparer should review and approve monthly reconciliations of other key accounts.
- Ensure original invoices are provided with any cheque before it is signed.
- Signed cheques should be mailed by a person who did not prepare them.
- Restrict access to blank unsigned cheques.
- All cheques, purchase orders and invoices should be numbered consecutively and you should regularly check for missing documents.
- Ensure accounting system users have individual access identification.

- Ensure that accounting software's built in controls, exception reports and audit tools are enabled and functioning and that their results are regularly reviewed.
- Mail should be opened by someone other than those responsible for record keeping.
- Deposits should be done by a person not in charge of accounts receivable
- The accounts receivable clerk should not be handling the original customer cheques but should be provided with copies.

Finally, since even the best system of checks and balances can be overridden or falsified, consider carrying sufficient fidelity insurance to protect against any significant losses through employee theft.

Ultimately, business owners need to trust employees. However, every business owner must also create an environment that protects the assets of the business.

Why and which employees steal from their employers

Generally, it is more often the younger employee under the age of 35 who steals from an employer, although older workers who do steal tend to take much more than their younger counterparts. Managers are the usual culprits for the worst cases of fraud. It's typically not the new-kid-on-the-block, but the long-term and trusted employee who ends up being the company crook. Often, it is someone who's been with a company for more than three years. Employees at private companies cause more losses than those at public or non-profit establishments.

There's an old saying that's long been accepted in fraud prevention circles called the 10-10-80 rule: 10 percent of people will never steal no matter what, 10 percent of people will steal at any opportunity, and the other 80 percent of employees will go either way depending on how they rationalize a particular opportunity. The good news is that there is much a business can do to sway this 80 percent to their side.

Another widely accepted theory is that of the late Dr. Donald R. Cressey called the "Fraud Triangle." According to this theory, there are three factors -- each a leg of a triangle -- that, when combined, lead people to commit fraud.

One leg is an individual's financial problem or need that they perceive is non-sharable; i.e., a gambling debt. The **second leg** is this individual's perception that there exists at the place of business an opportunity to resolve the financial problem without getting caught. The **third leg** is the individual's ability to rationalize or justify the intended illegal action ("After all I did for my company, they mistreated me. I was entitled to that money."). In shorter terms, PRESSURE plus PERCEIVED OPPORTUNITY plus RATIONALIZATION equals FRAUD.

Some key ways to prevent employee theft

- The first step to preventing employee theft is to screen job applicants thoroughly before hiring them in the first place. Background checks should be performed and should include a check on criminal history, civil history, driver license violations, as well as verification of education, past employment (including reasons for leaving), and references.

Consider running a credit check on prospective employees, as people with financial difficulties are more prone to fraud. In order to do this, you are legally required to notify the job applicant in writing that a credit report may be requested. You also need to receive the applicant's written consent.



- Studies show that the more employees believe they will be caught, the less likely they are to steal.

Be clear with employees that your company has zero tolerance for employee theft of any sort. This includes not only outright stealing, but also things such as taking a long lunch break without approval, using sick leave when not sick, doing slow or sloppy work, or coming to work late or leaving early.

Write and distribute a company policy that outlines exactly what constitutes stealing. Contact your local police department if you do discover an incident of employee theft so you send a message to your employees that stealing will not be tolerated.

Business owners and senior management must themselves be role models of honesty and integrity, or they may risk setting up a work environment that justifies illegal and criminal activity.

- Avoid at all costs allowing the finances of a business to be handled and controlled by a single individual. Separation of duties is critical, and no employee should be responsible for both recording and processing a transaction; i.e., don't allow the same person who sends out bills to collect the mail and prepare bank deposits.
- Run irregularly scheduled surprise audits or have a third party audit your books once a year. Also insist that your bookkeeper or any employee who has access to monies take a yearly vacation so you can examine their records.
- Make sure all checks, purchase orders, and invoices are numbered consecutively, and regularly check for missing documents.
- Use a "for deposit only" stamp on all incoming checks to prevent an employee from cashing them.
- Personally look into customer complaints that they have not received credit for payments.
- Most incidents of employee theft are revealed by coworkers, but many still are hesitant to report these incidents to their employers. Set up a system whereby employees may report employee theft anonymously. You may also want to consider offering rewards for informants while keeping their identity confidential.
- Unopened bank statements and cancelled checks should be received by the business owner or outside accountant each month and they should carefully examine for any red-flag items such as missing check numbers. They should also look at the checks that have been issued to see if the payees are legitimate, and make sure that the signatures are not forgeries.
- Require all checks above a nominal amount to have two signatures. Never sign a blank check. Sign every payroll check personally. Avoid using a signature stamp.
- Get an insurance policy that covers outside crime, employee theft and computer fraud. It will be there as a safety net in case your fraud prevention tactics don't work.
- Small business owners should take the time to review accounts payable by checking cash disbursements and payments. A very common scheme to look out for is billing-scheme fraud where an employee sets up fictitious "phantom" vendors.
- Be alert to disgruntled or stressed employees, or those who have indicated that they are having financial difficulties. Also look for any unexplained significant rises in an employee's living standards.
- A positive work environment has been shown to deter employee fraud and theft. Open lines of communication, positive employee recognition, and fair employment practices will assist in the reduction of occupational fraud.

