

## Embezzlement & Fraud: Is it Happening In Your Business?

Working with a lot of small businesses we have a good understanding how they handle the accounting and finance functions within their business. They have limited resources which makes most of the invoicing, bill paying, bank reconciliations, cash handling, and payroll processing handled by one, or maybe two people at most.

Unfortunately, the lack of resources to decentralize accounting functions are the reason small businesses have a disproportionate amount of embezzlement and fraud compared to larger businesses.

I was recently doing some research on this topic and was startled by some of the statistics compiled by the Association of Certified Fraud Examiners (ACFE) in their 2014 Report to the Nation:

- Small businesses are both disproportionately victimized by fraud and notably under-protected by anti fraud controls, a combination that makes them significantly vulnerable to this threat.
- The vast majority of occupational fraudsters (95%) are first-time offenders and 82% of fraudsters had never previously been punished or terminated by an employer for fraud-related conduct.
- The amount of time from when the fraud commenced until it was detected — for all schemes in our study was 18 months.
- The median loss per fraud scheme at small businesses is \$154,000.
- It takes time and effort to recover the money stolen by perpetrators. At the time of our survey, 58% of the victim organizations had not recovered any of their losses due to fraud, and only 14% had made a full recovery.
- Small businesses (defined as those with fewer than 100 employees) were victimized at 28.8%, which is the greatest percentage of all cases reported.
- Organizations with fewer than 100 employees face different fraud risks than larger organizations. For example, check tampering schemes occurred in 22% of small business cases, but only 7% of cases in larger organizations.

So while these are somewhat frightening statistics here are some cost effective suggestions small businesses can put in place to minimize their exposure:

Be aware and look around. Most fraudsters exhibit behavioral traits or warning signs of their crimes, such as living beyond their means or having unusually close associations with vendors or customers. In 92% of the cases at least one common behavioral red flag was identified before the fraud was detected.

Review and update your Code of Conduct policy in your handbook. If you don't have a hand book, create a separate Code of Conduct policy and review with all employees. This sets the expectation and consequences.

Educate your staff. Hold regular training sessions on basic security threats (online and off) and prevention measures for both new hires and seasoned staff. Promote and enforce the training by instituting policies that guide employees on the proper use and handling of company confidential information, including financial data, personnel and customer information.

Keep an open door. Tips, at 42.2%, are consistently the most common detection method for cases of occupational fraud. Of this total, your own employees accounted for nearly half of all tips received. So it's best to keep your door open and encourage open communication.

Insuring for Crime or Fraud: You can acquire commercial crime insurance which covers money, securities and other property against a variety of criminal acts, such as employee theft, robbery, forgery, extortion and computer fraud. Check with your agent on the cost and coverage offered by these policies.

Conduct Background Checks on New Hires: Hiring the right people can minimize the chance of fraud. While not full proof, with proper written consent this can give you some assurance there are no past criminal convictions.

Have a Manager Approve Expenditures and/or Sign Checks: While this may not be practical on all purchase or checks, set up a policy that say check over \$1,000 must be approved and/or signed by the owner.

Review Bank Register on a Periodic Basis: Again, this may not be practical depending on the number of transactions but have your accounting person print out, or send in a PDF file, your bank register every few weeks or every month. Take a moment to skim through and question anything that's not familiar. This process sends a message to your accounting department that you're watching and can be a powerful deterrent.

While you can't protect your business 100% from embezzlement or fraud, you can take steps that send a message through your organization on what is appropriate conduct. This sets both expectations and consequences. People are less likely to commit fraud if they know someone is watching them.

To read more, here is the link to the most recent ACFE 2014 Report to the Nation. <http://www.acfe.com/rtn/docs/2014-report-to-nations.pdf>