Fighting Fraud

A Short Guide for Small Businesses

Small businesses often have limited resources for fraud prevention programs. Yet, they are among the biggest targets for fraudulent activities with revenue losses related to employee-perpetrated fraud estimated at over $3 billion per year according to Canadian accounting associations.

The easiest way for any business with limited resources to deal with fraud is to put in place simple systems to prevent it in the first place. What amounts to very small steps can save a small business thousands of dollars and buy invaluable peace of mind.

YellowPages™

Internal fraud is fraud perpetrated from within the business by its employees. Unfortunately, this constitutes the most common type of fraud. Use the following tips to help develop a fraud prevention program for your business.

9 Steps to Prevent Internal Fraud

1› **Know your fraud risks**
Determine where your company's specific vulnerabilities lie in order to create and implement internal prevention controls.

2› **Employee background checks**
Check references, employment and educational history to ensure there's no previous history of fraud or illegal activity. If you're filling a position managing the company's assets, you may want to consider conducting a credit check with the authorization of the candidate.

3› **Ensure monitoring of cash situations and create system of checks and balances**
Have security cameras installed to monitor activity at registers and in inventory storage areas. Expenditures should always have a multi-step approval process consisting of a manager and an accountant to ensure validity of expense and to run the math. Additionally, key business functions should never be handled by a single employee, this makes fraud easier to conduct and to cover up.

4› **Conduct surprise audits**
If you do not have internal auditors, have your accountants periodically visit and audit specific functions of your business where fraud might occur. These audits are less designed to discover fraud and more to act as a deterrent as employees will know it will be more likely to be uncovered.

5› **Control the banking**
Small business owners should check bank statements themselves to avoid cheque tampering. Watch for missing cheques, cheques issued out of sequence, unknown payees, cheques which look altered, cheques not signed by authorized signatories, or any other unusual items. Conduct bank reconciliations once a month and consider using online banking tools if you regularly have many transactions and large dollar volumes.

6› **Use only approved vendors**
This can help fight billing schemes and phony invoices. A list of management-approved vendors should be available to all staff and this list should be routinely checked against invoices. Look for unknown vendors, vendor names similar to approved vendor names, vendors with no physical address or phone number or vendors with addresses matching an employee's address.

7› **Create and communicate your company's fraud policy**
Make all employees aware of what activities constitute fraud, the tools being used to combat it and the company's zero tolerance policy on fraud. Ensure employees know what to do and who to contact if they suspect fraud and be sure to inform employees about the actions the company will take if it is determined fraud has been committed. Often the communications themselves become a deterrent to fraudulent activities.

8› **Employee Assistance Programs**
Often internal fraud is committed by employees undergoing hardships who feel they have no other alternatives. An employee assistance program can help mitigate this risk and if a formal program is too expensive, institute an open door policy where employees can approach management for help when it is needed.

9› **Take action when fraud is discovered**
Obviously the punishment should match the offense but having a fraud policy is useless if you are unwilling to enforce it. Once small frauds are overlooked or permitted without repercussions, larger ones become possible. Consider options such as suspensions, demotions, salary cuts, probation, dismissal and legal action for differing levels of violations.

Preventing Common Types of External Fraud

Scams targeting small businesses range from strange office supply orders to fake invoices. Here's a short guide on common types of fraud and how to avoid them.

1› Fake domain name renewal notices

Be wary of unsolicited letters encouraging you to renew your website domain name or suggesting a new one.

- Check that the renewal notice matches your existing domain name. Watch for small difference like ".org" instead of ".ca" or missing letters in the web address.
- Check that the notice comes from the same company with whom you registered the domain name.
- Check your records for the expiry date of your existing domain name and see if this matches the notice.

2› Fake Yellow Pages directory listing or other unauthorized advertising

This type of fraud may be disguised as a solicitation for an update of an existing advertising product you have purchased or as an offer for a free listing when it is actually an order for a listing requiring payment at a later date. Other times, the communication may be disguised to look like it's from Yellow Pages when it actually isn't. For more information, **click here**.

3› Equip your front lines

Make sure your staff processing invoices or answering phone calls is aware of these types of fraud as they will often be the main points of contact. Always check that goods or services were ordered and delivered before paying an invoice.

4› Office supplies that were never ordered

Watch for invoices for goods you never ordered. Often this will be for items regularly ordered such as paper, printing or maintenance supplies. Keep records of all orders placed and check these against all invoices received. In some cases, you may receive phone calls which falsely claim to be from your "regular supplier" with a limited time or special offer. Supplies offered in these calls will usually be overpriced and of bad quality. Always deal directly with your supplier contact or directly dial your regular supplier to confirm this offer is indeed from them.

5› Be careful about your business information

Never give out information about your business information for advertising purposes unless you know how it will be used and you can confirm you are dealing with your standard advertising supplier.

6› Get it in writing

Never accept a business proposal over the phone. Always request the offer in writing and limit the number of people in your company who have the authority to approve purchases or create a multi-level approval process.

References

"Does Canada Have a Problem with Occupational Fraud?", Certified General Accountants of Canada, December 2011

Small Business Entrepreneurs: A Focus on Fraud Risk and Prevention, American Journal of Economics and Business Administration, 2011

Peak Small Business Center, "Preventing Fraud in the Workplace", Cary Christian, 2003

"The Little Black Book of Scams: Your Guide to Protection Against Fraud", Competition Bureau Canada, 2012

"Preventing Small Business Fraud", Carole Matthews, Inc., 2002

"How Companies of All Sizes Can Prevent Fraud", David Mielach, Business News Daily, November 2012

Who to contact when you suspect fraud

› **Competition Bureau of Canada**
1 800 348-5358
www.competitionbureau.gc.ca

› **Canadian Anti-Fraud Centre**
1 888 495-8501
www.antifraudcentre.ca

› **Better Business Bureau**
www.bbb.org

› **Yellow Pages**
1 877 909-9356

To get additional tips and find out more about digital marketing, visit:
businesscentre.yp.ca

YellowPages™