

Business Fraud Prevention Tips

as published July 8, 2009

Business owners are faced with making financial decisions on a daily basis. Do I buy this? Do I extend credit to that customer? Do I hire this employee? These decisions, if not made wisely, could impact your business, especially if someone has the intent to deceive or defraud you and your business.

To this end every business owner and financial manager should perform due diligence that prevents fraud and reduces employee theft. Some of these risks may include the risk of income loss relating to the extension of credit or hiring of new employees. Debtors can leave you stuck with unpaid invoices that result in cash flow shortages and an unscrupulous employee can rob you blind.

- Never extend credit to an individual or a company with whom you know nothing. Make inquiries, ask for references, and determine credit worthiness by obtaining a credit report. A credit report identifies exactly who you are dealing with and determines the credit worthiness of the applicant.
- Beware of phony invoices. Fraudulent companies send out solicitations for advertising and/or products in the form of invoices to trick businesses into paying without realizing that it is not an actual invoice and that they owe the sender nothing. All invoices should be approved for payment by those that incurred the expense and ultimately their supervisor.
- Make sure your administrative staff does not provide information about office equipment over the telephone so that you do not fall victim to the "Toner Phoner" scam in which fraudulent companies misrepresent themselves as your regular supplier to sell you over-priced office supplies.
- Ensure that you have a Privacy Policy in place (a legal requirement as of January 2004) and that the personal information of your customers and employees is secure. A shredder is mandatory piece of equipment for businesses so that any personal information or corporate documentation is not thrown in the garbage where thieves can retrieve it and use it to your or your customer's detriment.
- Retailers, be aware of individuals making credit card purchases for large ticket items where they appear to be in a hurry, don't ask questions and cannot produce any photo I.D. with the name that is on the credit card. And in particular, beware of the telephone order in which a credit card number is provided because despite the fact that you may obtain authorization from the credit card company; the fact that you don't have the purchaser physically in front of you so that you can obtain a credit card imprint and compare the signatures will result in the credit card company charging the item back to you if the credit card is subsequently reported as stolen or counterfeit.

- Do not deposit mail in a remote postal drop, especially checks which have been written to pay an invoice. Checks from these postal drops are being stolen with great regularity; they are altered to change the payee's name and the amounts are increased. Although you will be reimbursed by the bank if you discover the theft within a reasonable time frame, this can be a major inconvenience that you do not need. So always drop your mail at an inside postal drop.
- Perform a bank statement reconciliation at least once a month and preferably more often. If a check is stolen, lost or altered, you will be able to rectify the situation before it causes problems. You will also know if checks have been written on the business account that shouldn't have been and/or if the bank has made a mistake. There are many Individuals that have lost their businesses because they were unaware of the accounting practices conducted by a "trustworthy" employee.
- Know your employees; are they using your company vehicles and equipment to generate extra cash flow at the end of the work day? Do you have checks and balances in place to ensure that there is no internal theft of materials, money or time? Employee theft is a huge factor in the profitability of many businesses. Employee background checks are recommended for individuals that you are going to be trusted with company assets.
- Educate your employees; have a company policy so there is no doubt as to what is expected of them. Hold monthly meetings to discuss issues and problems and talk about the zero tolerance with respect to theft. If you as the business owner want to prevent fraud and theft from your company then you need to have a due diligence process in place that reduces risk. Again, know who you are hiring; pre-employment checks should be mandatory.

For more information on preventing fraud or if you believe you have a fraudulent situation you need rectified, contact Doug Sosnowski at dsosnowski@briscon.com.

Doug is a principal with Brisbane Consulting Group, LLC, a wholly owned subsidiary of Lumsden & McCormick. Doug has extensive valuation experience specializing in business valuations and litigation support services and is a certified expert in financial forensics. He joined Brisbane Consulting in 2005 with over 20 years of experience. Doug has earned numerous business valuation degrees including licensed in New York State as a CPA Accredited in Business Valuation (ABV); Accredited Senior Appraiser (ASA) as a member of the American Society of Appraisers; Certified Valuation Analyst (CVA) with the National Association of Certified Valuation Analysts (NACVA); and Certified in Financial Forensics (CFF) by the AICPA. He is a member of the AICPA and the NYSSCPA. Doug is active in the community as a board member with Community Services for the Developmentally Disabled and the Girl Scout Council of WNY. Doug graduated with honors from the State University of New York at Buffalo.