

The Business Owner[®]

Employee Fraud and Embezzlement

Stu and Betty were in their mid-70s, each with character lines beyond their years. Expressive lines that silently spoke of their long journey filled with experiences of hard work, joy and sorrow. I instantly fell in love with them. Their manufacturing firm, in its 35th year, did some \$2.8 million in annual revenue. As I listened intently to their story, they explained that they'd recently suffered their third bout of employee embezzlement—\$200,000 this time. They weren't sure they had what it would take to struggle through this time. They were emotionally exhausted and financially weak. Betrayed once again by a person they trusted, even nurtured.

Employee theft is white-collar crime. It's categorized by the FBI as deceit, concealment or violation of trust but not involving the application or threat of physical force or violence. These acts are committed to obtain money, property, or services; to avoid the payment or loss of money or services; or to secure a personal or business advantage.

Studies show that on-the-job theft is widespread and growing.

According to the 2003 National Retail Security Survey (NRSS), no other form of larceny costs American citizens more money than employee theft. U.S. retailers alone lost \$15.8 billion in 2003 to employee theft. That's not shoplifting, which is theft by customers and resulted in an estimated loss of \$10.7 billion in 2003.

The U.S. Chamber of Commerce estimates that U.S. employers lose \$20 billion to \$40 billion a year due to employee theft. Shockingly, the U.S. Chamber of Commerce states that 30% of all business failures are caused by employee theft, citing a report by David J. Shaffer and Ronald A. Schmidt.

"Occupational fraud and abuse is a tremendous problem, one that affects practically every organization," says the Association of Certified Fraud Examiners (ACFE). In their 2004 Report to the



continued on page 9

ALSO IN THIS ISSUE

Special Section: Employee Fraud

- The Fraud Triangle
- How to Avoid Employee Fraud
- Employee Has Embezzled. Should You Take Legal Action?
- What to Do If You Suspect Employee Theft
- Web Resources for Fraud Prevention
- Terms and Definitions to Know
- Warning Signs of Fraud
- Protect Your Intellectual Property!

- Tax Breaks Extended!
- Beware of Business Buyer Scams
- The Value of Customer Complaints
- Q & A: Quality of Financial Statements
- Survey Customers Without Invading Their Privacy

- Giving References for Former Employees
- Laugh a Little
- Ten Steps to Determining the Space You Need for Your Business
- Corporate Finance and Merger & Acquisition Expertise

D. L. Perkins, LLC
7010 S. Yale, Suite 120, Tulsa, OK 74136
918-493-4900 • 800-634-0605 • Fax: 918-493-4924
E-mail: info@TheBusinessOwner.com • www.TheBusinessOwner.com

From the Editor

Business is tough, but betrayal by one of your own takes the wind out of your sails like no other. Because most private businesses are thinly capitalized, loss of cash due to theft or fraud can take years to recover from. It can even put you out of business. In fact, an expert endorsed by the U.S. Chamber of Commerce estimates that 30% of all business failures are caused by employee theft. Shocking, but there is some good news: You can drastically reduce your vulnerability – starting today – by implementing and maintaining some basic strategies. The cost is nil and the time required is nebulous. Yes, big dividends and little cost. All that's required is that you read this issue of *The Business Owner*. Our feature topic is fraud prevention.



David L. Perkins, Jr.

What is that, you say? It won't happen to you? Please, get a hold of yourself! It's always better to be safe than sorry. Have you ever been fooled before? Of course you have. We all have. And it's not a matter of not trusting your employees. You simply must do what is prudent. They'll understand and assist you. Have your employees adopt the fraud prevention policy suggestions herein. Your honest employees don't want to be put in a position where they are tempted or accused. They'll also gain confidence in you, their employer, as you do what is wise and sensible.

Sincerely,

A handwritten signature in black ink, appearing to read 'D.L.P.', written in a cursive style.

David L. Perkins, Jr.
Publisher and Editor

TABLE OF CONTENTS

Special Section: **Employee Fraud**

- | | |
|----|---|
| 1 | Employee Fraud and Embezzlement
Risk Management |
| 3 | The Fraud Triangle
Risk Management |
| 4 | How to Avoid Employee Fraud
Risk Management |
| 5 | Employee Has Embezzled. Should You Take Legal Action?
Risk Management |
| 6 | What to Do If You Suspect Employee Theft
Risk Management |
| 6 | Web Resources for Fraud Prevention
Risk Management |
| 7 | Terms and Definitions to Know
Risk Management |
| 7 | Warning Signs of Fraud
Risk Management |
| 8 | Protect Your Intellectual Property!
Risk Management |
| 10 | Tax Breaks Extended!
Tax |
| 11 | Beware of Business Buyer Scams
Scam Alert |
| 12 | The Value of Customer Complaints
Marketing and Sales |
| 12 | Q & A: Quality of Financial Statements
Risk Management |
| 13 | Survey Customers Without Invading Their Privacy
Marketing and Sales |
| 14 | Giving References for Former Employees
Employees and Employment |
| 14 | Laugh a Little |
| 15 | Ten Steps to Determining the Space You Need for Your Business
Real Estate |
| 16 | Corporate Finance and Merger & Acquisition Expertise
Business Purchases & Sales |

SUBSCRIBER BENEFITS

Using the password below, log in to the members-only section at www.TheBusinessOwner.com for back issues.

Password for July 1 through August 31: **Fraud**

THE BUSINESS OWNER – EDITORIAL ADVISORY BOARD

David L. Perkins, Jr.
D.L. Perkins, LLC – President
Vercor – Partner
Editor and Publisher, *The Business Owner*
David@DavidLPerkinsJr.com

Trey Biggs - Marsh USA, Inc.
AREA OF FOCUS: Risk Management
trey.biggs@marsh.com

Dr. Wen Chiang – University of Tulsa College of Business
AREA OF FOCUS: Finance and Operations Management
wen-chyuan-chiang@utulsa.edu

Laura C. Conway, Attorney at Law – Porzio, Bromberg & Newman, P.C.
AREA OF FOCUS: Commercial and Insurance Coverage Litigation
lconway@pbnlaw.com

Dr. Jay Kent-Ferraro, Ph.D., President – Empowerment Technologies, Inc.
AREA OF FOCUS: Executive Coaching • Performance-Based Training
DrJKentFerraro@aol.com

Mark Gould, President – Gould Business Group • Partner - Vercor LLC
AREA OF FOCUS: Business Strategy and Analysis • Mergers and Acquisitions
mgould@gouldbusinessgroup.com

Matthew O. Henderson – Henderson Financial Group, Inc.
AREA OF FOCUS: Succession Planning • Employee/Executive Benefits
matt.henderson@gohenderson.com

Mark Jordan, MBA, President – Capital Strategies, LLC
AREA OF FOCUS: Mergers and Acquisitions • Business Valuation
mark@csinglobal.com

Bill Lohrey - Lohrey & Associates
AREA OF FOCUS: Taxation and Tax Accounting • Tax Law
wlohrey@lohrey.com

Armand Paliotta, Attorney – Hartzog Conger Cason & Neville
AREA OF FOCUS: Tax Law • Securities Law • Business Transactions
apaliotta@hartzoglaw.com

Jeffrey J. Presogna, CPA, CVA, President - Presogna & Company
AREA OF FOCUS: Taxation • Capital Formation • Valuation
jpresogna@aol.com

Steven Soule, Attorney at Law
Partner - Hall, Estill, Hardwick, Gable, Golden & Nelson
AREA OF FOCUS: Bankruptcy Law • Debtor/Credit Law
ssoule@hallestill.com

Jean Wilcox – Cattle Logos
AREA OF FOCUS: Marketing and Advertising
jwilcox@cattlelogos.com

This publication is owned and published by D.L. Perkins, LLC,
7010 S. Yale, Suite 120, Tulsa, Oklahoma 74136; 918.493.4900;
Fax 918.493.4924. Info@TheBusinessOwner.com.

David L. Perkins, Jr.
Publisher and Managing Editor

Cindy Vogel, Business Manager – cindy@thebusinessowner.com

Doug Ricks, Sales Manager – doug@thebusinessowner.com

Rena Williams, Marketing & Fulfillment Manager – renae@thebusinessowner.com

Kathy Piersall, A Blue Moon Arts, graphic design
Cover illustration: © Getty Images Photodisc

To subscribe, order reprints, private-label this publication or purchase articles for placement in your own newsletter, call 800-634-0605 or go to www.TheBusinessOwner.com.

Copyright © 2006 by D.L. Perkins, LLC. All rights reserved under International and Pan American Copyright Conventions. Reproduction, in any form, in whole or in part, is prohibited without written permission from an officer of D.L. Perkins, LLC. Issn. No. 0190-4914. Vol. 30, No. 4. Price \$199⁰⁰ per year.

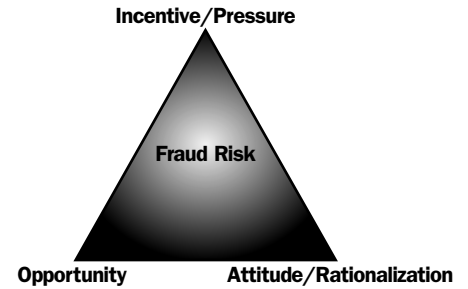
This publication is intended to provide general information on the subject matters covered. It is sold and distributed with the understanding that neither the publisher nor any distributor or advertiser is engaged in providing legal, tax, insurance, investment or other professional advice. The advice of a qualified professional should be sought before any reader applies a concept presented herein to his or her particular situation or business.

SPECIAL SECTION EMPLOYEE FRAUD

The Fraud Triangle

It is generally believed that three elements are found in almost every case of employee fraud. These elements allow people to commit fraud, and only when all three are present does fraud occur. The three elements are:

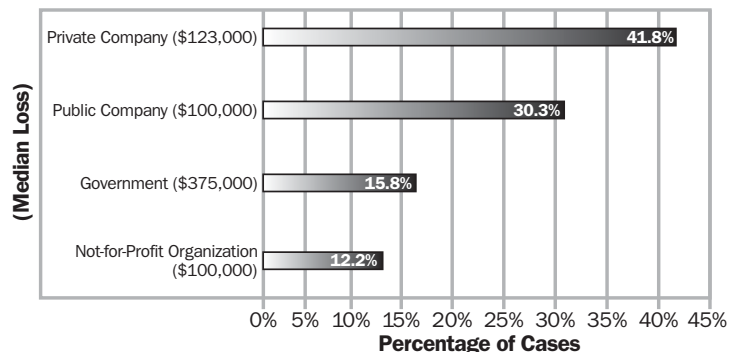
- 1. Opportunity.** For fraud to occur, the employee must believe he or she can both commit and conceal the crime. Unfortunately, seasoned expert Christopher Eiben believes that every opportunity to commit fraud will be exploited. The only question is when and how.
- 2. Incentive/Pressure.** Bearing down on a person. Often, it's financial. Pressure to display wealth beyond one's means or related to one's current or past expenditures. May stem from drug, alcohol or gambling addiction. Sometimes, it's emotional pressure—such as an extremely callous or cruel boss who instills in the employee a desire to “exact revenge.” Finally, job dissatisfaction or fear of losing a job also may create pressure that can lead to theft.
- 3. Attitude/Rationalization.** Most often comes in the form of “I deserve it.” In other words, the employee feels he or she is not getting what he or she deserves. Often it's an inflated sense of one's self-importance and contributions and a false sense of entitlement.



The second-most-popular form is totally different. It's the employee rationalizing his decision to take advantage of opportunity by saying “I'll just borrow it for a little while and then pay it back.” Although the “borrowing” may grow to hundreds of thousands of dollars, the perpetrator continues to rationalize his or her theft by “intending to pay it all back.”

Fraud prevention requires that owners and employees be alert to signs of any of these three elements, and that they move swiftly to root them out before they manifest themselves as fraud. □

Fraud Victims by Type of Organization



Source: Association of Certified Fraud Examiners

How to Avoid Employee Fraud

Fraud prevention expert Christopher Eiben says that to reduce the chance of fraud, businesses should at the very least “separate the money from the record keeping.” That means:

- A. Don't let the same person who receives and records receipts also book sales, generate invoices and reconcile receivables.
- B. Don't let the same person who approves purchases also pay for them (and the person who pays for purchases should be able to make a payment only when it is accompanied by appropriate approval documentation).

For very small businesses, achieving the above may mean the business owner must be involved in some of these tasks. For example, many business owners personally receive all incoming mail, stamp each check on the back with deposit information, and match daily check receipts with daily deposit totals.

Experts recommend that owners of small businesses directly receive (unopened) and review credit card statements and bank statements. Alternatively, have them sent to your accountant before they go to the bookkeeper.

As long as it is feasible, experts also recommend that business owners personally sign all outgoing checks and require expenditure-approving paperwork to be attached to each check submitted for your signature.

Here are more ideas for reducing your risk of employee theft:

- **Higher authority for higher check amounts:** If you don't personally sign all checks, require that you sign all checks over a certain amount. Make sure all employees, vendors and your banker know the policy and threshold amount.
- **Get preprinted checks with preprinted check numbers:** Keep track of each check by number and reconcile bank statements immediately on receipt.
- **Thorough employee screening:** Conduct thorough background checks, including personality profiles, on all employment candidates ... especially those that will hold senior positions or work in accounting or finance.
- **Annual review of credit report:** Check to make sure no unauthorized person has taken out a credit card in your company's name.
- **Insurance:** Consider purchasing bonding insurance, i.e., insurance against employee theft and fraud.
- **Use a payroll service.** Doing so will substantially reduce risk for theft of payroll tax funds.
- **Run a journal entry report every month:** The person who runs the report should not be the person who makes the entries. Go over any adjustments with the people who made them.
- **Investigate and approve all new vendors:** The owner should personally visit with the vendor or its representative.

Make sure the vendor is legitimate and not set up by an employee or someone in cahoots with an employee.

- **Watch for an increase in bad debts:** Similarly, watch for lengthening of the age of receivables. Personally investigate accounts that slow-pay or don't pay.
- **Mandatory vacations:** Require all employees (especially finance, accounting and management) to take at least a full week off per year. More important, don't allow paperwork to pile up during the break. Have someone else perform ALL of the regular duties of the vacationing employee.
- **Educate employees about the prevalence of employee fraud:** Make sure they're aware of the risk that employee fraud poses to the organization and internal controls that are necessary and prudent. Finally, educate them on the warning signs (see accompanying article “Warnings Signs of Fraud”).
- **Rotate jobs:** Periodically, have employees change jobs. Preferably, unannounced. This will substantially reduce the risk of fraud and also can raise employee satisfaction, uncover inefficiencies and dampen the hurt caused by unexpected turnover.
- **Periodic checks and surprise audits:** If employees know that their work will be checked randomly, they're much less likely to attempt to steal.
- **Promote and sustain an ethical culture:** Draft and ratify, as an organization, an ethics policy that clearly declares an expectation of ethical behavior at all levels of the organization ... and compliance with all applicable laws and regulations. Fraud prevention expert Christopher Eiben says, “Companies that countenance thievery will eventually be victimized by it.”
- **Don't tolerate abuse:** Persons who have addictions to drugs, alcohol or gambling have much higher incidences of deviance. Similarly, don't tolerate other forms of abuse at work such as verbal or sexual.
- **Create a confidential reporting mechanism.** Install a message box and encourage comments. Better yet, hire a service that will take calls and allow you to offer your employees an 800 number (“hotline”).

Separation of duties is the most fundamental, effective fraud prevention measure. No single employee should have complete control over an entire transaction, from writing checks to making deposits and reconciling statements. Ideally, a different person should handle each function. □

“If you are not making 50 mistakes a day, you are not trying hard enough.”

Dr. Robert Anthony

Employee Has Embezzled. Should You Take Legal Action?

You have indisputable evidence that an employee committed fraud against you and/or your company. You've terminated him or her. Should you take legal action? Press charges?

Emotionally and idealistically, of course you do. It's the right thing to do. Fail to do so and you fail to uphold your duty to society and fail to set a clear precedent at your business. Delinquents deserve to be punished. More so, they need to be punished. The more public the better. In fact, maybe we should go back to flogging in the town square.

Practically and realistically, on the other hand, some say "pressing charges" may not make sense. First, legal action is costly, stressful and time-consuming. Many would rather get the bad experience behind them. Second, it's likely an exercise in futility because the average amount reclaimed for U.S. white-collar crime is 20%. Forty percent recover nothing. Third, will a drawn-out fight damage company morale? Maybe it would be best for the company, and your family, if distractions were minimized and the incident swiftly put in the past. Fourth, Christopher Eiben, certified fraud examiner and author of *It Pays to Be Paranoid*, says many employers are culpable. They either harbored or tolerated an ethics-less culture or failed to maintain even a basic level of fraud prevention initiatives. He says even the most upright will go bad when faced with regular temptation.

What's right for you? It's a personal decision that you'll have to make based on the facts of your case and your own principles and priorities. As to the facts, here are a few to get you started:

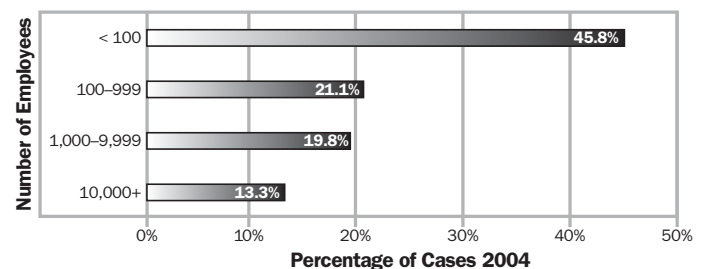
- **Call the police?** Doing so may be the right thing for you to do, but know that this has little real effect because the police are not going to make an arrest because you call and claim theft. Assuming they show up, it'll be a startlingly visible display for all to see. In addition, they can write a police report, something you'll almost certainly need to begin the process of pressing criminal charges. Finally, it doesn't cost you anything.
- **"Press (Criminal) Charges":** Pressing criminal charges is the act of requesting that the government (city, county or federal) protect your personal rights as a citizen – or those of your company, as a legal "citizen." In such a case, the government, through a district attorney or prosecutor, is the plaintiff. At the expense of the government, they will investigate the case and, based on their findings, decide whether to file charges. Once charges are filed, the case will be decided by a jury unless the defendant pleads guilty or the prosecutor and defendant work out a settlement beforehand. Compared to civil action, criminal prosecution is less expensive because the government represents you. But experts say that the injured party who pursues criminal prosecution typically will spend his or her own time and money assisting the government in gathering evidence. Criminal prosecution can take a very long time and the

terms of settlement are totally determined by the prosecutor (i.e., not by you).

- **File a (Civil) Lawsuit:** The civil court system is separate and distinct altogether from the criminal court system. It's a means by which a person or legal entity may seek protection or relief on his or her or its **own** behalf. You or your company will be the plaintiff, not the government. The good news is that you have the freedom to bring whatever claims you deem to have merit and you remain in control of any settlement terms. If it goes to trial, a judge or jury will decide. Civil remedies do not include incarceration. Civil trials are much more expensive because the plaintiff must bear all the expenses. It will be more expensive for the defendant as well because the government will not provide the defendant with an attorney.
- **Is it worth the time and money?** An attorney's dream is a wealthy plaintiff who pursues a weak case with irrational vengeance. Similarly, many judgments are awarded for money damages that are never collected. In these cases, is the favorable verdict enough to justify the time and expense? How much can you reasonably hope to recover if you win? These are important questions.

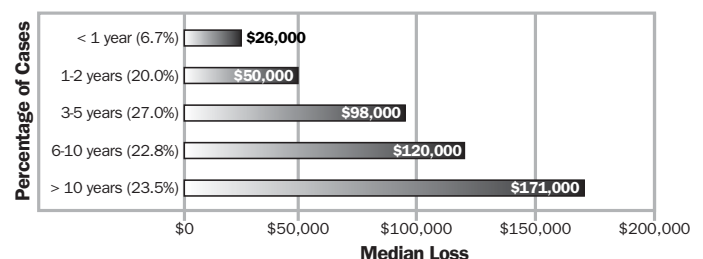
In summary, should you take legal action? Only you can decide. But as with anything, make sure you know why, what you hope to gain and what the cost will be. Legal action, whether civil or criminal, will take a very heavy toll on your time, money and emotions. Many who "win" end up with very little money and a lot of disappointment. □

Percentage of Cases Based on Size of Victim Organization



Source: Association of Certified Fraud Examiners

Tenure of Perpetrator



Source: Association of Certified Fraud Examiners

What to Do If You Suspect Employee Theft

If you suspect that an employee is stealing from you or your company, don't react immediately or emotionally. Take some time, gather your emotions, consult a trusted outside advisor and make a sound plan. In doing so, consider the following:

- 1. Don't accuse before you have factual evidence.** You don't want to make matters worse by getting into legal liability for the way you handle the matter. Don't tell anyone that such and such person did such and such. You could be sued for slander. Consult an attorney who specializes in employment-related matters.
- 2. Investigate.** Begin a thorough investigation. Hire a forensic accountant if necessary. If you can conduct it without others knowing, so much the better. If not, explain that you are looking into certain data and you would appreciate assistance where needed.
- 3. Find hard evidence.** Belief and suspicion are not fact. Are there witnesses? Are the witnesses credible? Do you, or they, have factual, indisputable evidence, or is it only circumstantial or interpretive? Are there documents or videotapes that could be obtained that render indisputable evidence?
- 4. Can I have a witness?** Have a management witness present at all conversations that you have with any of your employees.

- 5. Suspend before you fire.** If an employee behaves suspiciously or if there's credible evidence that an employee has engaged in or supported fraudulent activity, don't fire the employee. Place him or her on leave, paid or unpaid. Make your retain-or-fire decision after your investigation is complete.
- 6. Don't Detain:** If an employee refuses to talk or cooperate and attempts to leave, don't detain him or her against his or her will. Simply explain that if he or she does not provide information, you will have to make a decision without the benefit of his or her input.
- 7. Document, Document, Document.** Every step of the way, write down findings, keep notes and retain records. You may need them for evidence.

Keep in mind that you will likely be too emotional to manage the process objectively, professionally and effectively, so think hard about getting someone else to take the lead for you. □

"The thing you resist is the thing you need to hear the most."

Dr. Robert Anthony

Web Resources for Fraud Prevention

www.cfenet.com

Association of Certified Fraud Examiners (ACFE): Mission is to reduce incidence of fraud and white-collar crime, and to assist its 36,000 members in their efforts to detect and deter fraud. Provides anti-fraud training and education.

www.aicpa.org/antifraud

American Institute of Certified Public Accountants: Serving its members and the public since 1887.

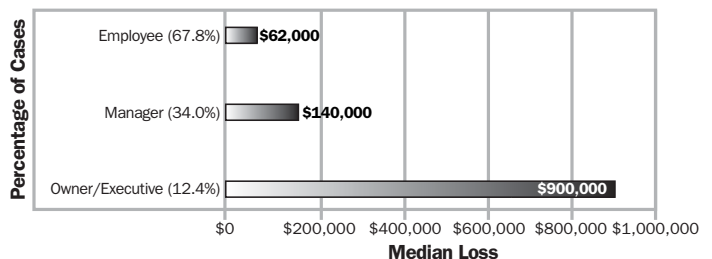
www.ckfraud.org

National Check Fraud Center: Private organization that provides information and intelligence to support in detection, investigation and prosecution of check fraud and white-collar crime.

www.bbb.org

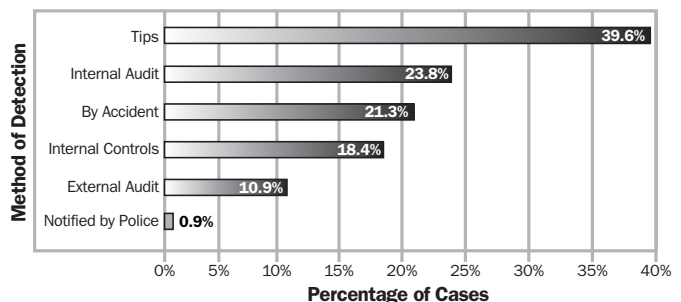
Better Business Bureau: Private, nonprofit organization developed to monitor and report marketplace activities to the public.

Position of Perpetrator



Source: Association of Certified Fraud Examiners

Detection of Fraud in Small Businesses



Source: Association of Certified Fraud Examiners

Terms and Definitions to Know

Embezzlement. Fraudulent appropriation of funds or property entrusted to your care but actually owned by someone else. May be carried out in a myriad of ways.

Revenue Diversion. A type of embezzlement that involves diversion of revenue (monies) away from intended beneficiary to alternate beneficiary. For example, an employee intercepts checks or wire transfers and diverts them to his or her own benefit. Typically, the employee then destroys related documents, entries or files, such as sales orders, to avoid detection.

Skimming. A form of revenue diversion (embezzlement) in which cash is stolen from an organization before it is recorded on the organization's books.

False Sale. The common factor is that the embezzler records only part of the sale transaction. Remember, two sets of transactions are recorded in a sale:

1. Financial sale (credit) and collection of cash or recording the debtor (debit)
2. Reduction of existing inventory in perpetual records (credit) and "cost of sale" entry in the records (debit)

The idea of this fraud/theft is to record reduction of inventory (the second part of the transaction) while not recording a sale. Employee takes the inventory for his or her benefit, records a transaction in the books that reduced the inventory but no sale is recorded and the business collects no money. When inventory items are large or have to be released or delivered from a storeroom, a false delivery docket is used to direct delivery or release of stock under what appears to be a legitimate sale. Computerized systems make these frauds more difficult but certainly not impossible.

False Purchase: False-purchase schemes are based on the theft of inventory before it is ever recorded in the company's books. The first part of the scheme is to order items to be stolen, and steal them at the point of receipt. A more sophisticated version is to have inventory delivered directly to another location by the supplier so that it does not even have to be moved from the premises.

The idea of the scheme is to record the financial side of the purchase so the supplier is paid, but not record receipt of items into inventory records. Purchased items thus are never missed and never recorded as received.

Bid Rigging: Fraudulent activity that may occur when a purchaser solicits bids to purchase goods or services. Bidders agree in advance who will submit the winning bid. The purchaser, which depends on competition between bidders to generate the lowest competitive price, receives instead a "lowest bid" that is higher than the competitive market would bear.

Fraudulent Disbursements: A type of fraud in which the perpetrator causes his organization to disburse funds through some trick or device.

- **Fictitious billing** is carried out by submission of a fictitious bill (invoice) to your company for payment of goods not provided or services not performed.

- **Check tampering** is conversion of an organization's funds by forging or altering a check on one of the organization's bank accounts, or stealing a check the organization has legitimately issued to another payee.

Check Kiting: Possible only when a person can write checks on and make deposits in two or more bank accounts. The check kiter takes advantage of "float," the number of days between check deposit and funds collection. Assuming that it takes three business days for checks to clear, a simple kite between two banks could be accomplished as follows:

On Dec. 1, a check in the amount of \$5,000 drawn on bank A is deposited in bank B. On Dec. 2, the check kiter cashes a \$5,000 check payable to cash and drawn on bank B with a teller at bank B. Because the original kited check will be presented to bank A on Dec. 4, the check kiter on or before that date will deposit a \$6,000 check drawn on bank B in bank A not only to ensure payment of the original kited check but to increase the amount of the kite.

As the process repeats, kited checks become larger, more cash is withdrawn, and the scheme continues until the shortage is covered or the kite "breaks" when one of the banks refuses to honor a kited check because funds on deposit are uncollected.

Kickback: Money paid illegally to gain concessions or favors. For example, an employee agrees to steer purchases or contracts of its employer to a certain vendor in exchange for cash payments or other personal benefits. □

Warning Signs of Fraud

- Unexplained drop in cash flow and profit.
- Increase in delinquent accounts and bad debt.
- Employee is defensive, emotional, territorial, protective and/or uncooperative.
- Employee unexpectedly and dramatically increases his or her personal expenditures, appears to have "come into money."
- Slow monthly closings (experts say accounting books should be closed within 10 days of month-end). □

"The greatest understanding you can have, if you want to become enlightened, is that no one will ever understand you."

Dr. Robert Anthony

Protect Your Intellectual Property!

Theft of confidential information and trade secrets can be just as damaging to your business as embezzlement. Information theft is a serious issue. Your intellectual property is one of the most important assets of your business. In the hands of others, your business may suffer greatly.

Case #1: David Olsen bought a sheet metal fabrication company and over many years put every nickel of his money and every ounce of his energy into making it a success. Over a long time he courted and finally secured a large convenience store company as a customer. He did so by designing a new fuel pump canopy that the store decided to adopt. It was a great account with the promise of many years of profitable business. But an employee—unaware of the proprietary nature of the designs and drawings—provided a copy to the purchasing agent of the customer. It was not long before the customer had found someone to make the canopy for a lot less money.

Case #2: Tom Wirt was a likeable person, a natural salesman quick to establish relationships. He became a valuable rainmaker for Bolder Engineering and made a very nice living. He began using company connections to forge personal business deals “on the side.” The owner tolerated it and it became, no doubt, a valuable perquisite of the job. But there was no stopping Tom’s climb. The day came when he resigned and started his own firm. He took a significant amount of Bolder’s business with him. It’s been six years and Bill Bolder will tell you—he would have been far better off if he’d never hired Tom Wirt.

What could David Olsen have done? Protect his valuable asset. How? By educating his employees on the confidentiality of the company’s intellectual property. By restricting employee access to drawings. By copyrighting each set of drawings and prohibiting copying of them. By closely tracking each set.

What could Bill Bolder have done? Require Tom Wirt to sign and maintain a strict but enforceable non-compete agreement. And possibly either letting Wirt go before his ability to damage Bolder rose to unacceptable levels and/or working out a long-term deal with Wirt that would prevent him from leaving. The main thing is, address the issue and take precautions before it is too late.

What about your company? Your intellectual property? Maybe you should take an inventory of your vulnerabilities and begin managing them properly. Here are some suggestions.

- 1. List and describe your intellectual property.** Ask yourself and your employees what information you have that is proprietary, sensitive and confidential? Who might have an interest in these data? If these data were to “get out,” what kinds of things could happen? How might this harm you, your customers or your vendors?
- 2. Use computer passwords.** Require your employees to use passwords to access your computers or network. This will serve to keep unauthorized people away from important files. Don’t let employees get lazy with their passwords—require they be changed monthly. Dissuade people from using features that “remember” passwords. This can make it easy for an unauthorized person to gain access to your system. Insist that users log off your network whenever they’re away from their desks, so unauthorized users can’t jump in from their workstations.
- 3. Have all employees sign non-disclosure agreements.** Make sure employees understand that theft of intellectual property is as serious to your business as theft of physical property. Use a non-disclosure agreement or a non-disclosure clause in an employment contract to spell out employees’ responsibilities for confidential or trade secret information. Be sure you define what your company considers confidential. This is critical, because it clearly differentiates which information belongs to your company and which belongs to the ex-employee. The agreement also should outline steps the employee must take to maintain confidentiality, such as using computer passwords, not removing sales lists from the premises, not copying documents to disk, etc.

continued on next page

About the Publisher



David L. Perkins, Jr. owns, writes, edits and publishes *The Business Owner*, the newsletter of choice for more than 35,000 paid

business-owner subscribers who are serious about building wealth through successful private business ownership.

Perkins draws editorial ideas and inspiration from his daily work as a merger and acquisitions consultant, where he has advised on more than 100 purchase/sale transactions involving both private and public companies. His M&A consulting firm is Vercor, which has 10 U.S. offices and a European affiliate. Vercor specializes in sell-side representation of businesses valued between \$5 million and \$50 million (see www.VercorAdvisor.com).

Perkins holds a BA in psychology from the University of Oklahoma and an MBA from the University of Notre Dame. He has formal training in business valuation. He also pulls editorially from prior experience in commercial real estate leasing and brokerage, commercial bank lending and private company financial management.

Perkins is the author of [*A Concise Overview of Business Valuation*](#) and co-author of [*The Business Sale, An Owner’s Most Perilous Expedition*](#). Both may be purchased at www.TheBusinessOwner.com.

Perkins is a professionally trained, content-rich platform speaker available for both keynote and breakout sessions. He is a Certified Toastmaster and a member of the National Speakers Association.

Protect Your Intellectual Property!, continued from previous page

4. **Keep tabs on your documents.** Set and enforce strict procedures for access to trade secret and confidential or proprietary information. Create a hierarchy of access among your employees for sensitive information. Allow only those who need certain information to see it. For example, a sales rep may need customer contact information for his or her territory. But the rep does not need your entire client list, and does not need access to billing data. Label key electronic documents (such as your customer database) as “read only” so they cannot be altered or written to disk.
5. **Don't tempt prying eyes.** Don't make it easy for people who aren't supposed to see confidential documents to snoop. Encourage everyone at your business to take certain basic precautions. Never leave documents lying around. File things away when you're done with them or when you're away from your desk. Lock your filing cabinet and your desk when you're away. Close computer files when they are not being used and never leave a file on your screen when you go away from your desk.
6. **Have a plan for terminated employees.** Don't let a disgruntled ex-employee become a security threat. Have a plan in place to keep a person from leaving your company with confidential documents. Some steps to follow include:
 - a. Have the person leave the company immediately upon termination. Letting an employee hang around a few days to get his or her affairs in order only invites this person to make off with papers and other information that might be valuable to your firm. Have a supervisor stand by while the employee removes personal possessions from his or her desk.
 - b. Make arrangement for immediate return of any confidential company information such as client lists, price lists, etc. Make the timely return of these documents a condition of receiving severance pay.
 - c. Insist that the person turn in keys both for the business premises and his or her desk and file cabinet. If he or she doesn't return them, change your locks.
 - d. Immediately sever the person's access to your computer network. This is especially important if the person can dial in to your network from home, and then simply log in and download important information.
7. **Buy cross-cut paper shredders—and use them.** Be careful when you are throwing out copies of sensitive or confidential documents. These include financial statements, proposals, customer information, reports, receipts, bills, invoices, etc. Don't just toss these in the trash. Shred them. Putting them in the garbage unshredded opens up a range of security issues. If your trash is not disposed of properly, these documents could easily end up in the wrong hands—or blowing down the street past prying eyes.

Are you serious about your business and long-term growth? Protect it from harm. Protect its intellectual property.

Employee Fraud and Embezzlement, continued from cover

Nation on Occupational Fraud and Abuse, they published the results of their study of 508 occupational fraud cases. In total, these cases caused \$761 million in losses. Here are some of their other findings:

No other form of larceny annually costs American citizens more money than employee theft.

Source: *NRSS*

- U.S. organizations lose 6% of their annual revenues to fraud.
 - Small businesses suffer disproportionately large losses due to occupational fraud and abuse. The median loss for small businesses was \$98,000—higher than the median loss experienced by all but the very largest organizations. Unfortunately, small businesses are less likely to be able to survive such losses and should better protect themselves from fraud.
 - Criminal background checks can help but will not weed out all fraudsters. Most frauds are committed by otherwise “honest” employees.
 - Recover of losses is very low. The median recovery is 20% of the original loss. 40% of victims recover nothing.
 - Confidential reporting mechanisms reduce fraud losses. The median loss among organizations that had anonymous reporting mechanisms was \$56,500 compared to \$120,000 for organizations that did not.
 - Among cases detected by a tip, 60% of tips came from employees, 20% from customers, 16% from vendors and 13% from anonymous sources.
 - Frauds detected by internal controls tended to be relatively small, with a median loss of \$40,000.
- Frauds committed by owners and executives caused a median loss of \$900,000—six times higher than losses caused by managers and 14 times higher than losses caused by employees.
- Most occupational fraudsters are first-time offenders. Only 12% had a previous conviction for a fraud-related offense.

30% of all business failures are caused by employee theft.

Source: *Shaffer & Schmidt*

Apparently, some experts weren't surprised by the ACFE's finding. “Family-owned businesses are more vulnerable to embezzlement ... because they're more trusting,” says Detective Steve Beck in an interview with *Family Business Magazine*. Beck is a white-collar crime investigator with the West Chester Township Police in Ohio.

continued on page 10

Employee Fraud and Embezzlement, continued from page 9

Amazingly, Christopher Eiben estimates that less than 10% of employee theft and embezzlement is ever discovered and less than 10% of discoveries are reported to authorities. Mr. Eiben is a certified fraud examiner and author of *It Pays to Be Paranoid*.

Family-owned businesses are more vulnerable to embezzlement.

What does this mean for you, the owner of a small or mid-size private company?

You are at risk!

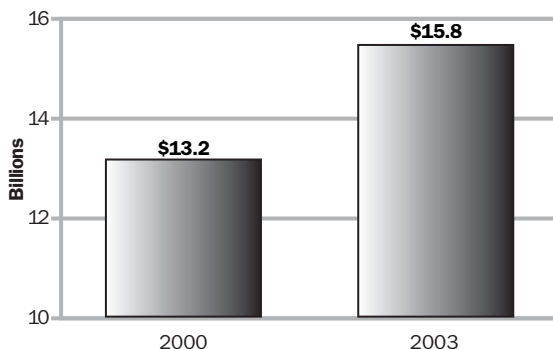
This does not mean you MIGHT be at risk. No. You ARE at risk. You must resist thinking "Oh, they'd never do that to me." The experts say every victim is shocked; betrayed by a person they trusted most. By a person they'd never have suspected in a million years. People who had given years of loyal and valuable service.

So get real! Installing and maintaining fraud prevention measures are part of what I call becoming a "real business." Yours is not a "real business" until you run it like one. □

Sources:

- "Beating Back Fraud," Business Finance Magazine, February 2006
- It Pays to Be Paranoid, Christopher Eiben
- "Safeguard Your Company Against Embezzlement," Family Business Magazine, Spring 2005
- "Experts See Theft on Rise in Workplace," The Oklahoman (date unknown)
- "Fight Fraud by Knowing Perpetrator, Common Scams," Research Recommendations
- "Fraud Wears Many Masks," Collections and Credit Risk
- "Combating Small Business Fraud," Regier Carr & Monroe, LLC Client Newsletter, December 2003
- www.AmericanExpress.com
- 2004 Report to the Nation on Occupational Fraud and Abuse," Association of Certified Fraud Examiners (ACFE)

Employee Theft (retail businesses only)



Source: National Retail Security Survey

Tax Breaks Extended!

President Bush signed into law on May 17 a tax relief bill that extends two tax breaks, provides a one-year "fix" for the alternative minimum tax (AMT) and modifies a few others.

AMT Relief: The new law provides substantial AMT relief by raising the amount of the AMT exemption to \$62,550 for joint filers and surviving spouses; \$42,500 for singles; and \$31,275 for married persons filing separate returns for 2006. The corresponding amounts in 2005 were \$58,000; \$40,250; and \$29,000. But without the new law, the amounts would have fallen back to 2000 levels: \$45,000 for joint filers and surviving spouses; \$33,750 for single taxpayers; and \$22,500 for married taxpayers filing separately. The bill also allows taxpayers to claim personal credits, such as the dependent care credit, against the AMT in 2006.

"The AMT has been the bugaboo of the income tax system for some time now, and ever since taxes were cut beginning in 2001, it has threatened to wipe out hoped-for tax reductions for many middle-class taxpayers," said CCH Principal Tax Analyst Mark Luscombe, JD, CPA. "This will shield about 15 million returns from the effects of the AMT at a cost of about \$34 billion. But then we go back to square one again for 2007."

Capital Gains, Dividend Provisions Extended: The law extends two investor-friendly tax provisions for two years beyond their scheduled expiration at the end of 2008. As a result, the long-term capital gains rate will remain at 15% until December 31, 2010, for taxpayers in all except the 10% and 15% brackets. For those in the 10% and 15% brackets, long-term capital gains will be taxed at 5% for the 2006 and 2007 tax years and at 0% for 2008-2010. In addition, dividends will continue to receive the same tax treatment as capital gains through the end of 2010.

"The extension aligns these provisions with many others that are due to expire at the end of 2010," Luscombe noted.

Capital Asset Purchase Incentives Extended: A break for small businesses, allowing them to expense up to \$100,000 per year in equipment, with the amount adjusted for inflation after 2003, has been extended through 2009. The inflation-adjusted amount for the expense deduction is \$108,000 for 2006.

IRA to Roth IRA Rollovers: Beginning in 2010, anyone can roll over an IRA to a Roth IRA. The ability to make such a rollover is currently limited to taxpayers with adjusted gross incomes of no more than \$100,000. The amount being rolled over must be included in gross income, so taxes will be due, but they can be spread over a two-year period if the rollover is made in 2010. Qualified withdrawals from Roth IRAs are not taxable and they're not subject to the minimum distribution requirements of conventional IRAs and 401(k)s.

"Kiddie Tax" Age Raised to 18: Under the so-called "kiddie tax" provisions, the unearned income of children under age 14 has been taxed at their parents' top rate, but on reaching age 14 they could file their own returns, which almost invariably led to their unearned income being taxed at lower rates. The new law requires that unearned income be taxed at parents' rates until children reach age 18. □

Source: CCH

Beware of Business Buyer Scams

If you're selling a business and it's going so smoothly it's spooky, beware! Some business buyers prey on inexperienced business sellers. Here's how one particular scam works.

You, the seller, receive a response on a "business for sale" ad you placed, typically on the Internet. The caller says he's with a private equity group (PEG) or small investment firm. You give him your data and receive a full-price offer. If you have representation, the buyer demands to work directly with you and not your representative. If you resist, the buyer says your rep is in the way, unprofessional, incompetent or unresponsive.

The terms call for purchase of stock rather than assets (very nice for you!) and payment in full within the first year, wherein more than half of sellers have to wait five to seven years. But there's very little cash at closing, maybe 10%. Not to fear; the buyer allows you to hold all the stock (i.e., equity shares) as collateral until you're paid in full. The terms call for the buyer to gain control of all the business assets at closing, including cash and accounts receivable.

The deal closes, you get the down payment and the buyer takes control of the company. The buyer then factors the receivables (i.e., sells them for cash), sells off the inventory, cleans out all the cash, maxes out the credit cards and pays no bills. Within a month or two, the buyer disappears. You're left with your collateral – the company – robbed of most of its assets and with huge liabilities.

One victim "sold" his company for \$1.8 million and the buyer skipped town after pulling out \$1 million. Also, the buyer persuaded the seller to let him (the buyer) take over the business with nothing down because "the funding was just a day or two late, but on the way."

According to various sources, if you get cold feet before closing and try to back out, these cons will try to extort money from you for not completing the transaction.

Think no one falls for this scam? Think again. Unfortunately, many have. At least two teams have been working this con in the United States for years. One team is a mother and two sons from the Midwest. Another is three men working together. The FBI arrested one of the ringleaders of this trio in Texas on March 3. His accomplices were arrested March 9.

If you encounter a similar situation, call the police or the FBI. Watch out for names such as Veneto Ventures, Fidelity Securities and Investments, James Robert Nance, Steven or Don Nadroski, and Jay Cohen.

Finally, stick to these recommendations when selling your business:

- Check the background of the buyer(s) extensively. Check references, pull credit reports, tax liens and litigation history, etc. Any litigation attorney will be skilled at this.
- Selling a business is tough. If the process is going spooky-smooth and/or the price and terms seem too good to be true, they probably are. Be cautious.

- If the buyer continually fails to meet deadlines and supply requested data, you have a problem. Don't accept excuses. Find a new buyer whose word is good.
- Don't let the buyer "work in the business" before he or she pays the cash.
- Require a substantial percentage of the purchase price up-front in cash before you turn over ownership. Seller financing is a fact of life in selling a private business, but accept no less than 50% in cash at closing.

When in doubt, hire a skilled representative. □

This article was adapted, with permission, from Ron Johnson's piece "Wanted—Considered Dangerous ..." that appeared in the International Business Broker Association Weekly Communication for March 14, 2006. Johnson is a business broker in San Ramon, California.

"Happiness is not leisure, it is victory."

Zig Ziglar

ORDER TODAY
2nd Edition

New
easy-to-read
format

**You'll learn
how to:**

- Build skills for assessing opportunity
- Accurately estimate investment options
- Make decisions that build value
- Save time & money

... and much more!

Concise Overview of
BUSINESS VALUATION
of Small and Midsize
Private Companies

For Business Owners, Managers and
Professionals Who Advise Them

DAVID L. PERKINS, JR.

Order now at
www.thebusinessowner.com/valuation,
or call (800) 634-0605.

The Value of Customer Complaints

Every business loses customers. And the tendency may be, especially for the small businessperson, to shy away from communicating with customers who walk away. But consider what a treasure chest of information lost customers hold. There's a reason those customers aren't buying from you. The reason may be benign. For example, they moved or their needs changed. But the reasons may be due to shortcomings in the way you do business or in the product or service they were buying from you. Wouldn't you like to know? Perhaps a minor correction would regain the customer. Surprisingly, many companies act as if they don't care.

Research shows that customers are twice as likely to complain when given a toll-free number. Customers are most likely to complain if asked what the problem was. And customers whose complaints were resolved effectively are more loyal than customers who never complained.

So, how easy do you make it for customers to complain? When you do get a complaint, what do you do with the information? Consider these 6 levels of complaint-handling maturity:

Level 1: No way to receive complaints.

Level 2: Don't respond to complaints.

Level 3: React to complaints and attempt to recover.

Level 4: Systematically respond to complaints and attempt to recover.

Level 5: Proactively solicit complaints and then systematically respond to recover.

Level 6: Proactively solicit complaints, systematically respond to recover, and then use the information to correct root causes.

Note that these are progressive. Your goal should be Level 6.

It seems counterintuitive to want to hear more complaints, but you should. We can get more complaints by simply requesting them and making it easy. Toll-free numbers and point-of-contact comment cards can work, but they're passive. Active solicitation of comments can best be done by contacting customers directly. Surveys after a completed transaction or scheduled meeting work best, depending on the nature of your business.

The key is to let the customer know that you want their feedback, and that you will act on it. This last point is key. If you don't provide service recovery and fix the underlying problem, the customer will be less likely to voice issues in the future. Also, remember to fix the problem and satisfy the customer. A small gesture, such as a handwritten note, can remedy an upset customer's attitude.

How well complaints are handled tells a lot about your management team. Managers who handle complaints with a positive attitude are likely to be the most successful in the long run because they recognize opportunities to improve. □

This article is substantially the work of Fred Van Bennekom, principal of Great Brook Consulting and author of Customer Surveying: A Guidebook for Service Managers. His Web site is www.greatbrook.com.



"So, as you can see, customer satisfaction is up considerably since phasing out the complaint forms."

© Mark Anderson, All Rights Reserved www.andertoons.com

Q&A: Quality of Financial Statements

Q: Can you explain the difference between Audited, Reviewed and Compiled financial statements?

A: Great question. Every business person should know the important differences:

Company-Prepared Statements: The statements that you print from your accounting software are neither audited, reviewed nor compiled. They are simply your internal financial statements. Are they prepared according to generally accepted accounting principles (GAAP)? When you receive company-prepared statements of another company, they should raise more questions than answers.

Before you rely on them, investigate how they were prepared. If you are not skilled at assessing company-prepared financial statements, get help.

Compiled statements: These are not any more reliable than company-prepared. Compiled simply means that somebody, typically an accountant, put them in a format that conforms to what financial statements are supposed to look like.

Reviewed financial statements. As the name implies, these have been "reviewed" by an accountant or accounting firm. Reviewed statements will include a letter from whoever did the review. Read it. Does it state that the reviewer found that the statements appeared to be prepared in accordance with GAAP? Or did the review give rise to doubts about the same? Regardless, keep in mind that a review is limited and does not guarantee accuracy.

Audited financial statements: Audited statements have undergone the most in-depth assessment by the reviewing person or firm. Similar to reviewed statements, they should be accompanied by a letter from the auditor. Read the letter. Is the opinion qualified or unqualified? If qualified, that means that the auditor is concerned about whether the statements were prepared according to GAAP and/or represent a fair picture of the company. An unqualified opinion means that the auditor believes the statements were prepared according to GAAP. As far as assurances go, this is the highest level. But (1) GAAP rules are complex and allow substantial "room to maneuver," so you'll still want to know exactly how certain transactions were booked; (2) if company officers wish to deceive, an audit might not uncover it; and (3) sometimes the auditors are biased and/or asleep at the wheel. □

Survey Customers Without Invading Their Privacy

For many businesses, engaging in customer research can mean walking a fine line between gathering vital information for you and intruding on the customer's privacy. It's a tough nut. You need to know who your customers really are and the reasons behind their buying decisions. But crossing the line to find out too much can be downright perilous.

"Staying out of customers' lives altogether takes away the ability to market effectively," notes Norman Scarborough, associate professor of business administration at Presbyterian College in Clinton, S.C. "But pursuing customers too aggressively or collecting unnecessary information will sour them faster than a glass of milk on a hot sidewalk."

That makes it essential to balance your needs with their right to maintain a level of privacy. Here are seven guidelines to help you tread that narrow line.

1. Decide first what you really need to know.

Many businesses approach customer information far too generically. They solicit across a broad swath, fishing for all kinds of data. That's a two-pronged mistake. For one thing, unnecessary research may cost you more. But just as important, you run the risk of spooking customers who worry you may be bullying your way into their privacy.

Start by identifying the information you'll genuinely need. If household income matters, include it. By the same token, if logistics are secondary, you can skip asking where your customers live.

2. Treat your research as you would any contact with your customers.

Researching who's buying your product, and why, doesn't mandate a complicated, foreign set of guidelines. Approach it as you would any aspect of customer service: Be forthright and ethical and conduct yourself in a manner that your clientele expects of you. "Treat your research as an extension of your customer service," says David Holtzman of GlobalPOV, a Washington, D.C., technology consulting firm. "If, for instance, the information you gathered leaked out, could you comfortably live with it? If you can, then you're OK."

3. Ask your customers for help and input.

If you want to balance adequate information with sensitivity to customers' privacy, talk to the folks whose privacy is in question. Prior to introducing customer research programs, arrange for a focus group or circulate a prototype customer questionnaire. Have them point out what's reasonable and what's too nosy. "It's always a good idea to test any survey on a small group before taking it full scale," Scarborough says. "Those taking the survey may interpret a particular question in a completely different way from what you intended."

4. Make it absolutely clear how you will use the information.

No client should be asked to share personal specifics unless he or she is told what the information is being used for.

If your business model calls for sharing the personally identifiable information that you collect, make it clear that there is a legitimate value proposition for customers providing you with their personal information. Post appropriate notice to them, such as in a privacy statement that can be found easily on your Web site.

Be sure to obtain their explicit consent to share their information with third parties, if your information-sharing plans go beyond what you simply need to do to fulfill customer requests, such as shipping them a product they ordered.

"There should be absolutely no surprises, like calls at 2 a.m. from someone you sold a customer list to," Holtzman says.

5. Tailor your methodology to your customers' comfort level.

Don't overlook the fact that your method of gathering information could be more intimidating than the data you seek. Find out in advance the best ways to make your customers feel comfortable passing along personal details about themselves. Some may be perfectly at ease filling out online customer profiles, while others may prefer a paper form and a Ticonderoga No. 2. Again, any way you can address customers' comfort level will imbue them with an overall sense of confidence that what you're asking them is justified and will be treated accordingly.

6. Make it quid pro quo.

Another effective way to balance information and privacy is a sense of equity between a business and its customers. Look into offering your customer base something of value in return for their willingness to share personal data about themselves. Try to make it substantive, such as discounts, specials that only they may be privy to, and other perks that may make them more at ease about giving out personal information. "Customers have a subjective sense about equity," Holtzman says. "If they give up something, they should get something. If they don't get that, eventually they're going to feel cheated."

7. Keep the information safe and, in time, get rid of it.

It goes without saying that keeping customer data secure is the very heart of a genuinely effective privacy program. So don't skimp on whatever safeguards you think are warranted. That covers everything from sophisticated firewalls and intrusion-protection software to reminding employees to lock cabinets at night.

Moreover, it's not necessary to keep customer data indefinitely. For his part, Holtzman suggests a "pull" date for information on customers who, say, haven't bought anything in a year or two. Not only does that further solidify a focus on privacy but also makes your customer information archives more manageable by weeding out outdated or worthless data. □

Jeff Wuorio writes about small-business management, marketing and technology issues and is co-founder of www.MyYawp.com, a Web site geared to producing superlative blogs and Web sites.

Giving References for Former Employees

Learn what to tell prospective employers about a former employee.

Whenever one of your employees leaves, you will have to decide what to say to other employers who call for a reference.

The decision is pretty straightforward if the employee left on good terms: You and your former employee can come up with a mutually agreeable statement to explain the departure. Or you can simply tell the whole glowing truth to any prospective employer who calls for a reference. But if the employee was fired, you face a more difficult task.

Defamation Lawsuits: The Fired Employee's Revenge

If you are not careful in your statements about former employees, you might find yourself facing a defamation lawsuit. To prove defamation, a former employee typically must show that you intentionally damaged his or her reputation by making harmful statements about the employee that you knew to be false.

At first glance, it might seem like only the most spiteful employer would get caught in this trap. But, if you make an unflattering statement that you don't absolutely know to be true, it could happen to you. Let's face it: Most reasons for firing make the employee look bad. And an employer often cannot prove what he or she strongly believes to be true – that an employee is stealing from the company, is incompetent, or lied about job qualifications, for example. An employer who makes such statements about a former employee could get into trouble. Your best policy is to say as little as possible and stick to facts you can prove.

What to Tell Other Workers

It can be challenging to figure out what to tell the rest of your workforce when an employee leaves on less-than-positive terms. Our advice: Don't go into detail. Shortly after an employee is fired, make a brief statement to your other workers, saying that the employee is no longer with the company. Tell them who will handle the tasks that person was responsible for, and ask them to direct any questions to you.

What to Tell Potential Employers

When a potential employer calls for a reference, you may feel trapped between wanting to tell the truth and fearing a lawsuit if you say anything unflattering. Unfortunately, this fear is not unfounded. The number of defamation lawsuits filed over negative references is growing all the time. And, even if your former employee can't successfully prove that you defamed him or her, you will have to spend precious time and money fighting the allegation.

Here are some tips to help you avoid problems:

- Warn a difficult employee that your reference won't be good. Yes, the employee should know this already. But you can avoid problems at the outset by stating the obvious: "I cannot provide a positive reference for you."
- Keep it brief. Some employers adopt a policy of giving out only dates of employment, job title, and final salary to prospective employers. If you choose to tell more, keep it to a minimum.
- Stick to the facts. Now is not the time to speculate about your former employee's bad qualities, or to opine on the reasons for his or her failure to perform. Limit your comments to accurate, easily documented information.
- Don't be spiteful. Many states offer some protection for former employers called upon to provide a reference. These laws generally provide that you will be shielded from defamation lawsuits as long as you provide information in good faith. This is a fairly nebulous legal standard, but it surely does not cover nasty or mean-spirited gripes.
- Don't give false flattery. If you had to fire a real bad egg (for example, a worker who was violent in the workplace or threatened coworkers), don't lie about it. You may choose to give only name, rank, and serial number, but, if you give a more expansive reference, don't hide the bad news. You may find yourself in legal trouble for failing to warn the new employer about these serious problems.
- Designate one person to give references. Choose one trusted person in your company to be responsible for all references, and tell all of your employees to direct inquiries to that person. Make sure that a record is kept of every request for a reference and every response, in case of later trouble. And you may want to adopt a policy of providing references only in writing, so you'll have proof of exactly what was said.
- Insist on a written release. If you want to make absolutely sure that you're protected against lawsuits, require former employees to sign a release – an agreement that gives you permission to provide information to prospective employers (and promises not to sue you for doing so). □

Reprinted with permission from the publisher, Nolo, Copyright 2006.

Laugh a Little

Six retired gentlemen were playing poker in Schaeffer's apartment when Jimmy Murphy loses \$500 on a single hand, clutches his chest and drops dead at the table. Showing respect for their fallen brother, the other five continue playing standing up. Michael Conner looks around and asks, "Oh, boys, someone's got to tell Jimmy's wife. Who will it be?"

They draw straws. Paul Gallagher picks the short one. They tell him to be discreet and gentle. Don't make a bad situation any worse. "Discreet? I'm the most discreet man you'll ever meet. Leave it to me."

Gallagher goes over to Murphy's house and knocks on the door. Mrs. Murphy answers and asks what he wants. Gallagher declares: "Your husband just lost \$500 and is afraid to come home."

"Tell him to drop dead!" says Murphy's wife.

"I'll go tell him," says Gallagher. □

Ten Steps to Determining the Space You Need for Your Business

Whether you're a small start-up or an established business, you should begin each search by carefully thinking through your needs. A clear understanding of what you do (and don't) want for your business will save precious time and money, commodities that you undoubtedly want to plow into the business itself. So before you hit the pavement or engage a broker to help you find the right spot, go through the points below and analyze what's most important to you in a business rental.

Before you plunge headlong into the search for suitable commercial space, think carefully about whether you really need to find space now. It may make more sense to run your business from your home. If you're just starting out in a business that doesn't require significant space or ready access to the public, maybe you can keep expenses low by working out of your house or apartment.

Or, if you're already renting space but looking to move, you might consider ways to improve your current lease situation and avoid the expense and inconvenience of relocating. Take another look at your lease – does it have an option clause, enabling you to expand into available space?

1. **Priorities.** If you're convinced that now is the time to move, think carefully about what you need, would like, and won't abide. Take out a sheet of paper and list items in three columns: "Must Have," "Nice to Have," and "Won't Have." Your goal is to end up with a concise statement expressed in words ("downtown area") or numbers ("maximum \$3,000 rent"). When you begin to consider available space, you can use this list to quickly and concisely evaluate its suitability.
2. **Rent.** The first issues to consider are the most obvious and, for many, the most important. Figure out the maximum rent your business can afford to pay per month. And if the landlord asks you to put down a security deposit before you move in, think about whether your reserves can handle a particularly big hit in the first month. Finally, consider how much money you can afford to spend to alter the space to fit your needs and tastes.
3. **Location.** The physical location of your business is likely to be important to you, your employees, your customers or clients, and/or your suppliers. The more people and groups you need to please, the smaller the number of possible rentals that will fit the bill. Consider the neighborhood, commuting time, and access to public transportation.
4. **Length of the lease.** It may be important for you to secure a space that will be yours for a long time to come – or you might want the flexibility of a shorter lease. Do you need to find a place right away? Or do you have the luxury of shopping around until you see the perfect spot? You need to assign a value – a priority – to the length of the lease and when it's available.
5. **Size and physical features.** Almost every tenant is concerned about the size of the rental. You'll want enough space, but to keep the rent down, limit the size to what you really need. You'll want the space to be well laid-out, comfortable, and welcoming to employees, clients, and customers.
6. **Parking.** For many businesses, it's essential to have ample parking – whether in a designated lot on the building site, on the street, or in a nearby parking garage. Parking may be a high priority for several reasons. If public transit is inadequate, people will need to drive to your business. If your business involves selling or servicing large items such as stereo equipment, customers will need nearby parking.
7. **Building security.** If crime is a known problem in the neighborhood and customers or employees are assaulted or robbed, you may be found partially responsible if you have not taken reasonable steps to prevent criminal incidents, or at least warn of them. Your landlord, too, may ultimately bear some responsibility, but the portion of a jury award or settlement figure that you end up paying is hardly the point. You never want to be in a position of worrying about customers' and employees' safety. So think carefully about the security of the neighborhood, and if you conclude that the risk is too high, look elsewhere.
8. **Image and maintenance.** The way a building looks – and how it's maintained – will be important to some and practically irrelevant to others. In general, the more your business serves the public, the more important is the building's appearance. If no one ever sees or visits your business, it may not matter much, except to you and your employees.
9. **Expansion or purchase potential.** If you plan on growing your business or would like to own your building in the future, you may want to rent space that has the potential for expansion or purchase. You'll save yourself the hassle and expense of another search and move to new space, and you may be able to lock in favorable expansion or purchase terms now, in your lease. Look for a lease with an option to renew or an option to buy.
10. **Neighboring tenants.** It may be important to be in a building with certain types of tenants – for example, businesses that complement yours or provide a needed service. Lawyers, for example, may want to locate in a building where there are accountants or title insurance providers. Healthcare professionals may want to be near a hospital, pharmacy, or lab. Whatever your business, you may want to find a building that houses a health club, coffee shop, or a fast copy service that you, your employees, or customers will find handy. □

Reprinted with permission from the publisher, Nolo, Copyright 2006.

VERCOR

"Expertise for *The Business Owner*"



**"I'm sorry, Jim, I'm afraid this is only
a win win situation."**

- ◆ ***Business Seller Representation***
- ◆ ***International Transactions***
- ◆ ***Mergers & Acquisitions***
- ◆ ***Debt & Equity Finance***
- ◆ ***Acquisition Assistance***
- ◆ ***Strategic Buyer Search***
- ◆ ***Management Buyouts***
- ◆ ***Pre-Sale Planning***
- ◆ ***Growth Capital***

Serving Companies with
\$5 million + in Annual Revenue



800.634.0605 · www.VercorSC.com · Confidential@VercorSC.com

THE BUSINESS OWNER
7010 S. Yale, Suite 120
Tulsa, OK 74136

ADDRESS SERVICE REQUESTED

DATED MATERIAL

PRSR STD
U.S. Postage
PAID
Documation