



Mistaken Identity

Are You Vulnerable to Identity Theft?

By Eileen Cohen, CPA, Partner

Spring has arrived and you finally resolve to do something about all the clutter. You toss out the pre-approved credit card applications, ancient bank statements, bills and charge receipts. You finally give away that old computer. You're feeling back in control, but you may have just allowed that control to be stolen. You've made yourself vulnerable to identity theft.

Last year, according to the Federal Trade Commission, there were over 45,000 complaints of identity theft in California alone. Identity theft victims may spend thousands of dollars and months or even years trying to clear their names and their credit after thieves have trashed them. The most important thing is to be vigilant about *all* your personal information.

Prevention Tips:

1.) **Never give out your personal information – by phone or email – if you're not absolutely certain of the identity of the person requesting it and why he**

or she needs it. Thieves may pose as someone calling or emailing from your bank or credit card company in order to get your information. Identity thieves may even pose as the IRS requesting information.

2.) **Safeguard your documents and mail.** Shred all documents that contain any personal information. Pick up new checks at the bank rather than having them mailed to your home. Keep your eye on cashiers while they have your credit card; be sure they're not making a second copy, or "skimming" the information.

3.) **Be smart about passwords and PINs.** Don't write them down, memorize them. Don't use common identifiers as passwords or PINs, such as



If you discover or suspect that you're a victim of identity theft, act quickly – time is of the essence.

your birth date, mother's maiden name, or the last four digits of your Social Security number or phone number. The most secure passwords contain a mix of letters and numbers.

4.) **Keep track of when bills and statements should arrive.** If a bank statement or credit card bill is late, contact the company right away. A thief may have submitted a change-of-address form on the account.

5.) **Monitor your credit report.** The three credit agencies (Equifax, Experian and TransUnion) are required to give you one free report each year. To order a report, visit www.annualcreditreport.com, or call toll-free (877) 322-8228.

CONTINUED ON PAGE 2

Is something missing from your bottom line?

By Mary Ayers, CPA, Manager



We are all too familiar with the mega fraud scandals of Enron, Tyco, and WorldCom. And just about every day you can pick up any newspaper and read about how fraud happened in another company. But what about your company? Could it happen to you? The answer is YES. Virtually every business will be a victim at one time or another. And smaller businesses are more likely to be victimized than the largest companies.

According to the Association of Certified Fraud Examiners' *2004 Report to the Nation*, embezzlement and other forms of fraud occur at a higher rate in small businesses than in larger businesses. About 46% of fraud occurred in companies with less than 100 employees, whereas 30% occurred in public companies. The median loss experienced by small businesses was \$98,000. This was higher than the median loss by all but the very largest organizations. Small businesses are less likely to be able to survive

CONTINUED ON PAGE 2

IN THIS ISSUE:	PAGE
• Mistaken Identity/Are You Vulnerable To Identity Theft?	1
• Is Something Missing From Your Bottom Line?	1
• Client Profile/John Nava	3
• Clients In The News	4
• From The Managing Partner	4

Mistaken Identity CONTINUED

What to Do If You Are a Victim:

If you discover or suspect that you're a victim of identity theft, act quickly – time is of the essence. Take the following steps in order to clear up your credit and your name:

- **Place a fraud alert on your credit report, and review your credit reports for additional errors.** A fraud alert will help prevent a thief from opening more accounts in your name. Contact the fraud hotlines for one of the three agencies; they are required to then contact the other two. (See **HOT TIPS**)

- **Close any accounts to which you think a thief may have access.** Call the companies' fraud departments right away, and send any documentation you have by certified mail. Use the ID Theft Affidavit, available online at the Federal Trade Commission site: www.consumer.gov/idtheft.

- **File a report with the local or state police, and the Identify Theft Registry.** California's Identify Theft Registry is a centralized database to verify that your identity has been stolen. Find more information about the registry at <http://ag.ca.gov/idtheft>.

- **Take steps to correct the false information on your credit report.** See complete guidelines for action in *Take Charge – Fighting Back Against Identity Theft* at www.consumer.gov/idtheft.

- **File a complaint with the Federal Trade Commission.** Your report will assist the FTC in their efforts to stop identity theft. You can file online or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338).

- **Contact NSBN.** We need to be aware of the situation and can advise you on steps to take.

While identity theft is a growing threat for everyone, following the steps outlined above will reduce your vulnerability. The key is to be conscious always of the value of your personal information, and the importance of safeguarding it.

Eileen Cohen may be reached at efc@nsbn.com or (310) 288-2272.

CREDIT REPORT HOT TIPS

For your free annual credit report, contact:
www.annualcreditreport.com or call toll-free (877) 322-8228.

To order additional credit reports/credit fraud hotlines:
• Equifax: (800) 685-1111/(800) 525-6285; www.equifax.com
• Experian: 888-EXPERIAN (888-397-3742); www.experian.com
• TransUnion: (800) 916-8800/(800) 680-7289;
www.transunion.com

To opt out of receiving offers of credit in the mail,
call: 1-888-5-OPTOUT.



Is something missing from your bottom line? CONTINUED

such losses and should exercise greater caution and vigilance in protecting themselves.

Why Are Small Businesses At Higher Risk?

Two key reasons small businesses are more vulnerable to fraud, primarily embezzlement, are the lack of segregation of duties and a higher level of trust placed in employees. While it is important to cultivate a collegial working atmosphere, be careful not to create a breeding ground for fraud. While most of your employees are trustworthy, sometimes things happen to an otherwise honest person – family medical bills, personal debt, gambling losses, drug or alcohol addiction, loss of social status – and the thought of “I’ll just borrow it and return it later” creeps in. Given the right circumstances, some individuals may eventually act on that thought and your profits will begin to seep out the door.

How Can You Prevent It?

Embezzlement is a special type of fraud. It involves the violation of your trust and the misuse of company assets for one's own personal gain. You trust your employees to pay the company bills, to properly account for inventory, or deposit customer receipts. But when an employee starts paying bills to a fictitious vendor, pilfering inventory, or skimming customer receipts, your trust is violated and your profits begin to dwindle.

The best way to safeguard your company's assets is to recognize and improve weaknesses in your internal control practices. It is also vital that you exercise management oversight.

What are Internal Controls?

Internal controls are the company's policies and procedures that are designed to provide

reasonable assurance that the company's assets are safeguarded, the financial information is accurate and reliable, and that the company complies with laws and regulations. The success of any internal control system is in monitoring the controls to ensure they are working as intended.

The internal controls required by your business will depend on the type and size of the business. A retail store, for example, may focus its efforts on protecting inventory with security cameras and performing surprise inventory counts. A manufacturing company with many hourly employees might concentrate on preventing time card fraud by using a mechanical time stamp machine.

Regardless of your industry, you must protect your business. Part of the creed of the Association of Certified Fraud Examiners is, “Fraud is Easier to Prevent than to Detect.” A proactive approach to preventing fraud is a must in today's business world.

If you would like more information regarding proactive fraud controls for your business, please call Mary Ayers. She can be contacted at mea@nsbn.com or (310) 288-4294.

What Can You Do?

Doing the following can help reduce the incidence of fraud (this list is not all inclusive):

- Develop a fraud policy that outlines what actions you will take if an employee commits fraud. Be sure the policy is communicated to every employee.
- Conduct background checks on prospective employees. The background check should include screens for criminal records as well as financial problems.
- Perform regular cash reviews that reconcile receipts and disbursements.
- Regularly verify assets, including inventory and supplies.
- Never sign blank checks.
- Segregate duties; related duties should be assigned to different people.
- Rotate job duties periodically.
- Review and monitor employee computer access to financial and sensitive company information.
- Regularly review the vendor listing; i.e. know who your vendors are.
- Provide a hotline that can be used anonymously by employees, customers, or vendors to report suspicious or known fraudulent activities. Be sure to follow up on all allegations.
- Periodically the business owner should open and review the bank statements, checking the payees and endorsements.