

from Chuck's Desk

Accounting

Income Taxes

Business Consulting

Specializing in the Training and Consulting in the Use of QuickBooks Accounting Software

Winter 2003

Visit My Web Site: www.affordabl.com



In This Issue

Keep Identity Thieves Out of Your Life

Volume 5 No. 4

from Chuck's Desk

is published periodically during the year by **Affordable Business Services, Inc.**
8105 N.W. 58th Place
Fort Lauderdale,
FL 33321-4520

Tel. (954) 720-8750

Fax: (954) 720-1913

E-Mail:

cdonovan@bellsouth.net

Web Site

www.affordabl.com

I welcome any comments or suggestions you may have.

Please call or e-mail me at your convenience.

If you do not wish to receive my newsletter, please let me know by e-mail or telephone and I shall remove your name from our mailing list promptly.

Chuck Donovan

Keep Identity Thieves Out of Your Life

I was in California recently. **Everywhere - in the newspapers, on television and radio, and on billboards – were warnings to protect yourself against someone stealing your personal information.** I was not aware that the misuse of personal information is such a severe problem. However, I have found out it has become one.



Identity Theft is on the rise and expected to increase in the coming years. Many millions of people became victims of the crime during the past few years and its out-of-pocket costs have exceeded \$1.5 billion since January 2001.

Criminals can commit it easily due to lax credit industry practices and the ease of obtaining Social Security numbers. Federal authorities often misclassify the crime. As a result, thieves have about a 15% chance of being caught.

The Crime of Identity Theft

The crime occurs when a thief steals Social Security numbers, driver's license numbers, credit card numbers, ATM cards, telephone calling cards, date of birth and other pieces of a person's identity. He uses this information to impersonate the victim, spending as much money as he can quickly before moving on to another one.

There are two types of identity theft.

"Account takeover" occurs when the thief gets hold of a person's existing credit account information and purchases products and services using either the actual credit card or the account number and expiration date. The victim learns his account has been taken over when he receives his monthly account statement.

"Application fraud" occurs when the thief uses a person's Social Security number and other identifying information to open new accounts in the victim's name. The victim does not learn of application fraud for some time, because the monthly account statements are mailed to an address used by the thief. **Surprisingly it is a friend, relative, or co-worker who is the thief in about 20% of the cases.**

We Must Be Concerned!

In September of this year the Identity Theft Resource Center and the U.S. Federal Trade Commission disclosed in separate surveys that **nearly 10 million Americans were victims of identity theft during the previous twelve months.** It was an 80% increase from the previous twelve month period. 25% of all victims indicated their credit cards, checkbooks or social security cards were lost or stolen.

The surveys revealed startling facts. Nearly 85% of the victims found out about their identity theft in a negative manner. Only



Affordable Business Services, a full service accounting firm, offers innovative business solutions to small and medium size companies through specializing in the training, and consulting in the use of QuickBooks business management software.

Chuck Donovan MBA brings over 20 years of financial expertise to the business having worked as a senior financial executive with firms ranging in size from \$20 million to \$3 billion in sales.

His broad, hands-on accounting and finance experience has taught him that financial information must be more than just a series of numbers.

He shows and helps business owners to use their financial information to increase their cash flows, improve their profits, and build their companies, so they can plan for a secure future.

A QuickBooks Professional Advisor and experienced problem solver, Chuck is a graduate of Dartmouth College and received his MBA from American International College.

15% found out due to an action taken by a business. A large majority indicated the opening of a credit card or the takeover of a card account was their first indication of a crime.

Others discovered new accounts had been opened, apartments or homes rented, medical care obtained, or employment sought in their name. ***The emotional impact of the crimes was equal to that of violent crime victims.***

Although ***many victims did not know how their personal information was obtained,*** most learned when their credit was severely damaged or they were turned down for a job or loans, tried to buy a home or a car, or were arrested for crimes they had not committed. The personal information was also used to obtain government documents and misused on tax forms, existing credit card, checking, and savings accounts.

Although ***a victim is generally not forced to pay the thief's bills,*** he is left with a bad credit report and spends months and even years regaining his financial health. He finds the people whom he must deal with lack sensitivity to his situation. He also gets little help from the authorities as he tries to untangle the web of deception that has allowed a thief to impersonate him.

Common Ways to Steal Information

Stealing wallets is the best way for a thief to find Social Security numbers, driver's licenses, credit card numbers and other pieces of identification.

Thieves are now using more sophisticated means:



- ***searching through trash bins and trash*** for unshredded credit card and loan applications and documents containing Social Security numbers.
- ***stealing mail*** from mailboxes to get newly issued credit cards, bank and credit card statements, pre-approved credit offers, investment reports, insurance statements, benefits documents, or tax information.
- ***posing as an employer, loan officer, or landlord*** to access a person's credit report fraudulently
- obtaining names and Social Security numbers from ***personnel or customer files*** in the workplace.
- ***"shoulder surfing" at ATM machines and phone booths*** to obtain PIN numbers.
- Finding personal information on ***Internet sources*** such as public records sites and fee-based information broker sites.

The Latest Way

The most recent one, called "phishing", uses the Internet. The thief imitates a financial institution's Web page or e-mail to deceive the victim into submitting his name, Social Security number, account numbers, and passwords.

While it is simple, the consequence for an unsuspecting victim is devastating ranging from depleted accounts to a destroyed credit rating.

There are three different ways of doing so.

1. The victim receives an email that looks as if it comes from a real financial

institution. The message has a "Sender" field reading "CustomerService@Financial Institution and asks the recipient to send personal information.

2. The thief creates an imitation Web site of a financial institution complete with its logo and similar language. In an e-mail the victim is requested to click on a link opening the imitation Web site and submit personal information.
3. The thief tries to gain unauthorized access to the victim's computer by sending a message to it with an IP address indicating that the message is coming from a financial institution.

Could You Become a Victim

So how do you know if you could become a victim of someone stealing your personal information. ***You might if any of the following situations apply to you.*** You



- get several offers of pre-approved credit every week and do not shred them.
- do not shred banking and credit information before throwing them away.
- carry your Social Security card in your wallet.
- do not have a Post Office Box or a locked, secured mailbox and use an unlocked, open box at home to drop off your outgoing mail.
- give your Social Security number whenever asked without learning how it will be safeguarded or give it orally without checking to see who might be listening.

- have your Social Security number and/or driver's license number printed on your personal checks.

Golden Rules to Reduce Your Risk

The following are golden rules you should follow to help reduce your risk and ensure your personal information is protected:

- purchase a ***paper shredder***, become more security-aware in document handling, and question why people need your personal information.
- install a locked mailbox at your residence and ***mail your bills and other sensitive mail inside the post office*** rather than putting them into outside mail boxes to prevent mail theft.
- ***review*** your credit card, bank and telephone ***statements*** carefully each month for unauthorized use.
- ***photocopy*** all credit cards, bank accounts, and investment ***data*** and place the copies in a secure place so you can quickly contact the companies if anything happens.
- ***do not carry*** extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse.
- ***do not have*** your Social Security number or driver's license number ***printed on your checks*** nor allow merchants to write either one on your checks.
- ***take credit card receipts*** with you always and never toss them in a public trash container.
- ***create passwords that combine letters and numbers*** rather than using the last four digits of your Social Security number, mother's maiden name, your

birth date, middle name, pet's name, or consecutive numbers that a thief can easily discover.

- **avoid giving out** your Social Security number, credit card numbers or other **personal information** over the telephone, by mail, or on the Internet unless you have a trusted business relationship with a company and you have initiated the call.
- **be suspicious** of any e-mail seeking personal information and never give out your Social Security number, PIN, or account numbers by e-mail.
- **do business with companies that provide transaction security protection** and have strong privacy and security policies, when shopping online.
- **avoid** giving your bank, credit card companies, insurance companies, and investment firms **the right to sell or share your financial information**.
- **remove your name** from the marketing lists of the three credit reporting bureaus - Equifax, Experian and Trans Union - to reduce the number of pre-approved credit offers.
- **order your credit report** at least once a year from each of the three credit reporting bureaus to check for errors and fraudulent use of your accounts.



If You Become a Victim

If you think you are an identity theft victim, immediately contact the Federal Trade Commission which is responsible for receiving and processing identity complaints and file a complaint. There are affidavit forms on its Web site and instructions on what to do such as contacting credit agencies and filing a police report.

Keep detailed records of your case. Write down the names of those with whom you discuss your problems and the dates you spoke to them. Follow up your discussion in writing by certified mail. If you must send documentation to creditors, such as a police report, keep the original and send a copy.

Lastly, set up a system to track your case, so you can find information when you need it. Keep everything relating to the case even if it has been resolved. Credit errors have a nasty habit of reappearing.