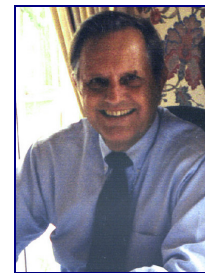


from *Chuck's Desk*

Affordable Business Services Inc.

www.affordabl.com

In This Issue

- GAO Audits IRS Security of Taxpayer Data
- Protecting Your Good Name

Volume 7 No. 2

"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

We are on the Web!
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

Hardly a week goes by that we do not hear or read about another company putting thousands of consumers at risk of identity theft because it has lost sensitive data. Recently a hacker gained access to the personal files of forty million accounts at an Atlanta firm processing credit card and other payments for banks and merchants.



Name, date of birth, address, social security number, financial information, driver's license number, bank account number, and credit card numbers are among some of the information readily available to an outsider through these security lapses.

A database that a hacker would surely love to get access to is the Internal Revenue's. It is a juicy target. The Service is well aware of this and concerned about **IRS data security**. It has gone on record stating it considers the confidentiality of the taxpayer data a priority and monitors its mainframe systems closely.

Identity theft is not limited to someone hacking into a major database. There are countless other frauds and scams – all designed to obtain our valuable personal information through fraud and deception for economic gain. These crimes will become more common and the lawbreakers more daring as electronic transactions become widespread in the coming years.

The recent theft of the personal information affects every one of all ages. **Protecting your good name** is critical. A little caution is necessary on all of our parts. Identity theft is a subject worth staying current on.

GAO Audits IRS Security of Taxpayer Data

The Government Accountability Office (GAO) has conducted two audits of the IRS's security of its taxpayer database during the past three years and found security gaps and weaknesses existing that need improvement.

The GAO reported in April that the IRS could very well be included among Citigroup, Bank of America, DSW Shoe Warehouse, ChoicePoint, and LexisNexis as organizations having data security troubles. **The agency needs to improve its security operations** according to the GAO report.



The report did say that the **IRS is making progress fixing security holes** in the systems it operates, but is not keeping up with new exposures and threats. **By not keeping pace with them the IRS could expose sensitive taxpayer financial data to unauthorized individuals.**

The GAO audited the IRS in 2002 and made the latest audit between February and October 2004. This current report said the IRS needs to improve controls over its financial and tax processing systems and to finish the work on correcting the weaknesses found in the earlier audit. To date the Service has fixed 32 of the 53 from 2002. The GAO has now

Affordable Business Services offers accounting, income tax, and consulting services to individuals and businesses.

The **full service accounting firm** offers also innovative business solutions to small to medium size companies through specializing in the training, and consulting in the use of QuickBooks business management software.

The firm's principal **Chuck Donovan MBA** brings over 25 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.

Financial information is more than a series of numbers. The firm focuses on explaining and teaching the business owner to use the data to make more money and improve the business.

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

added 39 new weaknesses to the list.

Among these weaknesses are perimeter security, disaster recovery plans, adequately securing access to the mainframe computers, and preventing unauthorized access to the IRS network.



The latest audit also found that the IRS does not keep taxpayer data separated from the data in the Financial Crimes Enforcement Network (FinCEN). The latter is a system used by federal law-enforcement agencies and the IRS to investigate financial crimes. As a result, anyone with the right to use the IRS's mainframe systems could get into FinCEN and conversely law enforcement could gain access to taxpayer data.

GAO mentioned that ***too many users can see too many types of information within the IRS's systems*** and considered this to be a significant security gap. The IRS must allocate its data control privileges correctly to cure this gap.

Many of the weaknesses outlined in the 2004 audit are present because the IRS does not have an Internet Threat security program in place throughout the Service. The audit recommended the implementation of security policies and procedures, training of employees with security responsibilities, and information security testing and evaluation of its systems.

All audits require a written response. Acting Deputy Secretary of the Treasury Arnold Havens indicated the ***IRS has tightened up access control on its mainframe systems, is fixing the remaining security weaknesses, and put a plan into action last year to improve the security at all of its centers. These actions are scheduled for completion by the end of this year.***

Protecting Your Good Name

We tend to think that seniors are the most likely group to be preyed on and have their identities stolen over the Internet. Their general inexperience with computers and the Internet would make them a prime target for hackers, hijackers and other bad guys just waiting to steal their identification, passwords, and financial information.

However, ***college students and young adults are also prime targets of identity theft.*** Their lack of worldly experience and innocence causes them to be less careful and makes them easy victims. Colleges are well aware of the threat to their students and caution them constantly in the information being distributed to the students.



Old-fashioned Fraud and Theft

These schemes have been around for centuries. All can not succeed without the willing participation of the victim. The bad guys prey upon a victim's basic desires — profit, money, gratification, advancement, or anything else the schemer can identify that will attract a potential target.

Many of the ways someone can wrongfully obtain and use your personal data subjects may be familiar ones, but well worth reviewing again to assure you are up to date on the latest schemes.

Most Common Schemes

The most common ones the bad guys use are:

- **Theft of Business Records** - They steal the victim's information from files in businesses where he is a customer, employee, patient or student. They may also bribe an employee who has access to the files or hack into the business's computer files.
- **Shoulder Surfing** – They stand next to a victim in a checkout line and memorize his name, address and telephone number while he is writing a check. They also do it by standing near a public telephone and watching the victim entering telephone or credit card numbers.



- **Dumpster Diving** - They search through personal or business trash and landfills for personal records.
- **Under the Color of Authority** - They pose as an employer or landlord to obtain the victim's credit reports.
- **Skimming** - They use a special data collection and storage device to get credit and debit card account numbers as the card is processed at a restaurant, store or business location.

Phishing and Spoofing Scams

A growing number of bad guys are using the Internet to steal a person's identity. **Phishing and Spoofing frauds make victims think they are getting an e-mail from a good source or valid web site which is not so.** These scams are very successful.

The criminals have pretended to be companies and organizations such as AOL, MSN, Earthlink, Yahoo, PayPal, eBay, Best Buy, Discover Card, Bank of America, Providian, and the IRS to scam victims.

- **Phishing** – It is **an expression** coined by hackers to mean **"link alteration"**. A victim's response is transferred to another e-mail address subliminally connected through linkage to the original one.

A criminal pretends to be a legitimate company sending cleverly forged e-mail messages to tempt victims to validate account information by providing key personal data and sharing passwords and credit card numbers.

The bad guy trusts that a victim will believe the message is from a valid company with whom they are doing business and is not a piece of junk mail. The message instructs a victim to answer it either by a return e-mail, by filling out an e-mail form, or by clicking on a link to the criminal's web site.

- **Spoofing** – The e-mail **appears to come from someone or somewhere other than the criminal.** It is sent to deceive a victim into opening the message and convincing him to submit the personal and financial information requested. It is generally used to commit credit card and bank fraud.



Other Devious Ways

In addition to the above schemes and scams there are several other ways for a criminal to obtain a victim's personal information.



Stealing is a very common way. Whether it is the ***theft of wallets and purses*** containing identification and credit and bank cards, the ***theft of mail*** containing bank and credit card statements, pre-approved credit offers, new checks, or tax information, or ***breaking and entering*** the victim's home to obtain personal information, the criminal will use any crafty method to get his hands on the information he needs to perpetrate the fraud.

Once he has such knowledge of victim - name, date of birth, address, social security number, financial information, driver's license number, bank account number, or credit card numbers, ***he is ready to use it*** to:

- Buy expensive items with the credit and debit card account numbers,
- Open new credit card accounts,
- Change the mailing address on credit card accounts to mask his purchases,
- Take out loans to buy automobiles, boats, and other expensive items,
- Establish telephone or cell phone service, or
- Counterfeit checks and debit cards.

The frauds are done for the criminal's personal economic gain.

Devastating For the Victim

Identity theft can be devastating for a victim. It often requires months and maybe years to straighten out the problems created when the victim's identity is stolen and to restore it to what it was before the theft occurred.

Clearing his good name will take long hours of closing bad accounts, opening new ones, and repairing a credit record wrecked by the fraud. He may also have to pay significant out-of-pocket expenses in the process of doing so. There may collateral issues in terms of the impact on jobs, loans, education, and housing.