

ADDING VALUE

Volume 4: Edition 3

Third Quarter 2005

SUMMARY:

Your Personal Information: What It's Worth

Data brokers are businesses that compile and sell personal information to marketers, creditors, employers, private investigators, and virtually any other party that can prove it has professional interest. What the brokers charge for personal data varies. But here are some examples of what different pieces of information can fetch when served up à la carte by major commercial data vendors.

- Date of birth: \$2.
- Address: 50 cents.
- Social Security number: \$8.
- ZIP Code: 50 cents.
- Marital Status: \$7.95.
- Employment information: \$13.
- Education history: \$12.
- Published phone number: 25 cents.
- Unpublished phone number: \$17.50.
- Cell-phone number: \$10.
- Driver's-license information: \$3.

Figures courtesy of Preemptive Media. For more information, go to www.preemptivemedia.net

A special thanks to Detective Richard Staaf, Mt. Lebanon Police Department, for his advice in the preparation of this newsletter.

ADDING VALUE is mailed quarterly to our clients and friends. The intent of this publication is to share some of our more interesting views and research with our clients.

WRIGHT ASSOCIATES

Third Quarter Investment Review and Outlook

Identity Theft

Social Security cards, driver's licenses, credit cards, bank account statements, birth records, and other personal documents are frequently requested in the ordinary course of business. With the advent of the Internet, it becomes increasingly convenient and sometimes necessary to provide the information on-line. Unscrupulous scamsters are finding ways to steal your personal information in increasingly pro-active ways. According to the Federal Trade Commission, identity theft is the fastest growing crime in the U.S. Last year over 10 million, or 4.6% of the population, were victims of some form of identity theft. The FTC also reports that 42% of all complaints received in 2004 were concerning identity theft. Here's our take on the subject, with some thoughtful pro-active action that all consumers can avail:

Schwab's commitment to Account Protection

First, Schwab, as a registered broker-dealer, is subject to the rules and regulations of the Securities and Exchange Commission ("SEC") and other regulatory agencies. Specifically, Schwab adheres to SEC Rule 15c3-3, which is designed to safeguard your cash and securities. All assets at Schwab are held in a SEC-approved depository. These assets are maintained free of any direct or indirect lien and cannot be used by Schwab for any purpose. Second, Schwab is also required to be a member of the Securities Investor Protection Corporation (SIPC), the assets you custody with Schwab are insured by this entity. Under SIPC, clients of a failed brokerage firm receive all non-negotiable securities registered in their names. To the extent that SIPC cannot recover securities owed to a client, funds from a SIPC reserve are available to satisfy the remaining claims up to a maximum of \$500,000 per "client capacity". This figure includes a maximum of \$100,000 on claims for cash. SIPC reports that 99.7% of eligible investors have been made whole in the 306 failed brokerage firm cases that it has handled over the past 32 years. Third, additional account protection is provided by Schwab through Lloyds of London, up to an aggregate of \$600 million. In simple terms, what this means is that there are several layers of control at the broker-dealer level to protect you against failure of Schwab to protect your assets. In the past 32 years, only 0.3% of investors had claims in excess of the SIPC limits. It is a remote possibility that any client of Schwab would lose their assets through theft.

Personal information reported to Schwab on Applications

Second, Schwab as a registered broker-dealer and Wright Associates as a registered investment adviser also have requirements enacted by the SEC to protect your privacy and the privacy of any personal data reported to either company. We protect confidentiality, we shred information, we protect computers with passwords, we update virus protection, we set-up firewalls, and we back up computers. Schwab requires numerous safeguards to prevent any unauthorized withdrawals from your accounts. If any administrative process seems cumbersome for the withdrawal or transfer of funds, remember it is for your protection. But most of all, we use common sense.

Things to do before your identity is stolen

Third, there are steps to take to protect your personal information. The U.S. Department of Justice suggests adopting a “need to know” attitude to your personal data. Your credit card company may need to know your mother’s maiden name so that it can verify your identity when you call to inquire about your account. However, a person who calls and says he is from your bank does not need to know that information if it is already on file with your bank. Richard Staaf, a detective in the Mt. Lebanon, Pennsylvania, Police Department, told us that it is critical to protect your social security number combined with your date of birth. With these two pieces of information, an identity thief can gain access to your bank accounts, credit accounts, utility records, and other sources of personal information. Here are some other strategies to protect your personal information:

- Don’t give it out unless you are absolutely convinced it is required or to your benefit.
- Consider putting your work phone number on your checks instead of your home phone number. If you have a P.O. Box, use that instead of your home address. If you do not have a P.O. Box, use your work address.
- Pay attention to your Social Security Personal Earnings and Benefit Statement. The Social Security Administration mails it each year about three months before your birthday. Check the information. If incorrect information is recorded, contact

the Social Security Administration immediately. Someone may be using your Social Security Number for employment purposes. The number is 1-800-269-0271.

- Do not sign the back of your credit cards. Instead put “Photo ID required.”
- Check your homeowner policy. Identity theft protection coverage is now included in many policies to cover expenses of up to \$5,000 for the following activities: acquiring credit reports to research fraudulent activity, wages lost due to time spent away from work to re-establish credit, attorney and court fees for removing judgments, application costs for re-filing loans denied due to identity theft, fraudulent withdrawals from certain financial accounts, and miscellaneous costs such as phone calls, postage, and photocopies.
- Periodically check your credit report for suspicious activity.
- Freeze your credit report. This offers the most protection, with some more strings. First, laws are only in effect in 10 states (none of our clients live in these states) and states charge a \$20.00 fee each time you freeze or unfreeze your credit report paid to the credit bureau. Still, the beauty of the system is that only you can freeze or unfreeze the account.
- Sign up for on-line bill payments. Surprisingly this is more secure than sending paper with a stamp. As long as your computer is protected with a firewall and virus software, online banking and bill paying may reduce your risk of data theft by reducing the number of people that have access to the account. Remember, it is not the computers that steal information, it’s human beings.
- When you do pay by check, do not put the complete account number on the FOR line. Instead use only the last four numbers. The credit card company knows the rest of the number, and anyone who might be handling your check as it passes through all the check processing channels won’t have access to it.
- Buy on-line with credit cards, not debit cards. With a credit card you have maxi-

mum liability for unauthorized purchases of \$50.00.

- Don't respond to "phishing" email. This looks like a message from a company you do business with and warns that you will be terminated if you don't update or verify your financial information within 24 hours. Don't click on these links.
- The U.S. Postal Service suggests individuals deposit outgoing mail at a Post Office or blue collection box or give it directly to your letter carrier. Identity thieves can steal your outgoing mail from your mailbox, especially if you have raised the mailbox flag to signal the carrier that there is outgoing mail to pick up. Incoming mail is also vulnerable. Thieves can complete a "change of address form" to divert your mail to another location. Always question a sudden drop in mail delivery.
- Buy a cross-cut-shredder and destroy all unsolicited pre-approved credit offers and blank courtesy checks.
- Try to add passwords to online and offline accounts, so impersonators need more than names, addresses and social security numbers to impersonate you.
- Don't use your mother's real maiden name or your city of birth as identifiers.
- Refuse to give up your social security number. Be aggressive about guarding your current number. Never have your SS# printed on your checks. (DUH!) You can add it if it is absolutely necessary.
- Right now. Go to a copy machine and place the contents of your wallet on a photocopy machine. Do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. Carry a copy of your passport when traveling either here or abroad.
- Use a Uniball 207 pen to sign checks. The ink in this pen cannot be washed off a paper check.
- Always keep the toll free number on your credit card handy, and separate from the card. Call immediately if you cannot find your credit card.

National Credit Bureaus

There are three national credit bureaus in the United States.

Under a 2003 federal law, consumers are allowed one free credit report per year from each of the three national credit bureaus, effective in September 2005. Some consumer advocates say that ordering a report from a different bureau every four months is an adequate method of checking one's credit. To order a free report, you must go to a central website (www.annualcreditreport.com), call 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

It pays to be a little cynical with companies that are using the promise of free credit reports to deceive consumers into registering for a subscription credit monitoring service. Indeed, while Experian admitted no wrongdoing, it recently agreed to give up nearly \$1 million and refund customers in settlement of a U.S. Federal Trade Commission lawsuit. Wells Fargo, which has experienced various data breaches since 2003, launched a \$12.99 per month plan last year, while Bank of America, which lost non-encrypted data tapes containing information on more than a million federal account holders last December, now sells a \$129 yearly monitoring program. Spokesmen say that "credit monitoring services and past problems with data security, should be viewed "as two separate issues." As Detective Staaf pointed out, rather than preventing the problem from occurring, the marketplace is responding by trying to profit through services like credit monitoring and identity theft insurance. What's really needed is prevention and control. Do business only with those banks and credit card companies who have adequate controls and are working closely and proactively with law enforcement to prevent identify theft.

In the worst case scenario

Things to do if your identity is stolen:

- If data is stolen, place an "extended fraud alert" on your credit report by calling one of the three consumer agencies. Equifax 1-800-525-6285, Experian 1-888-397-3742 and

TransUnion 1-800-680-7289. This alert remains for seven years, and requires creditors to contact you if anyone wants to open an account in your name. You are also entitled to two free credit reports within 12 months.

- Close the account that you know, or believe, has been tampered with or opened fraudulently. Notify credit card companies and banks in writing. Certified mail with a return receipt requested will provide documentation.
- File a report with your local police in the community where the identify theft took place. Get a copy of the police report or at least the report number to aid in dealing with creditors who need proof of the crime.
- If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try the state police. You can also call your state Attorney General's office (see www.naag.org for a listing).
- Detective Staaf, of Mt. Lebanon, also recommends that ID theft victims complete an ID Theft Affidavit which was developed by the Federal Trade Commission.
- File a complaint with the Federal Trade Commission. The Identity Theft and Assumption Deterrence Act of 1998, which made identity theft a federal crime, also directed the Federal Trade Commission to track identity theft complaints and provide a resource for victims of identify theft. By filing a complaint, you will provide information that can help law enforcement officials across the nation track

down the ID thieves. It also helps the FTC to coordinate efforts with other government agencies in stopping fraud and ID theft.

- Document all conversations; keep copies of all correspondence, follow up in writing all resolutions to the problems.
- Keep the FTC website address handy www.consumer.gov/idtheft/, it is the most credible, unbiased source of information on identity theft.

In closing, in researching this article, we have come to the conclusion that everyone is vulnerable to identity theft and our vulnerability is increasing daily. The best offense is vigilance and a strong defense.

Finally, if you want to read a book on one of the world's best scamsters, now reformed and legitimate, Frank Abagnale's book, [The Art of the Steal](#) is highly recommended. He opines that it takes only 20 "clicks" to steal anyone's identity anywhere in the world.

Sincerely,

[Kathleen S. Wright, CFA](#)
[A. Gregory Lintner, CFA](#)

[Wright Associates](#)
[1500 Oxford Dr., Suite 230](#)
[Bethel Park, PA 15102](#)
[412-854-2100 \(PHONE\)](#)
[412-854-2550 \(FAX\)](#)