FISHER FINANCIAL
STRATEGIES

Financial Strategies

FALL 2006

Welcome to the inaugural issue of *Financial Strategies*. This newsletter is intended to help you manage your household's finances. Our Fall 2006 issue is on identity fraud.

This is a topic with which I have had considerable experience, having been an identity theft victim – twice. I hope that some of the information here is news to you and that it assists you in reducing your own exposure to ID theft. I'd really appreciate receiving your feedback on this newsletter. Please let me know if it was helpful.

I also value your input for topics that you'd like to see in future issues of *Financial Strategies*. I had initially intended to discuss ways to avoid online ID fraud in this issue, but it soon became clear that a proper discussion of "low-tech" fraud would easily fill the available space. Since only about 10% of identity thefts are attributed to online losses, I decided to save that topic for a later issue.

Consider the following scenario: A criminal drives through subdivisions in mid-afternoon, scanning the houses. She's looking for homes with mailboxes accessible from the street, no cars in the driveway, and other indications that no one is at home. Each time she finds one, she stops. Sorting through the mail, she removes credit card offers and returns the remaining mail. Later, she completes the credit applications, changing the addresses to various locations to which she has access. New credit cards are issued, and it will be weeks or months before her victims know what's happened to them.

This might sound far-fetched, but it actually happened; a former colleague of mine was one of this woman's victims. Happily, there was no lasting damage to my friend's credit and the thief was later caught.

Not all ID theft victims get off so easily, though. Some spend 30 to 50 hours repairing damage done to their credit records. In some of the worst cases, the identity of the victim is used as an alias by a thief who's later arrested for some other crime. A criminal record is created under the name of the ID theft victim, who then becomes subject to arrest [1].

ID THEFT - HOW COMMON IS IT?

Accurate statistics for ID theft are hard to come by, but a study reported by the Bureau of Justice Statistics found that 3% of US households had at least one member who had been a victim of ID theft during a specified six-month period. It found that about two-thirds of households experiencing ID theft reported monetary losses. One in four victims did not even know that they *were* victims until they were contacted about late or unpaid bills. The Federal Trade Commission estimates that over the course of a 10-year period, you have a one in ten chance of experiencing serious identity theft.

Your confidential personal information can be compromised in surprising ways. In 2005, the Boston Globe reported that some real estate documents held in registries of deeds across

[1] "But, Officer, That Isn't Me," by Kristin W. Davis, http://www.kiplinger.com/personalfinance/magazine/archives/2005/10/idtheft.html

Massachusetts contain the Social Security numbers of property owners.[2] To make matters worse, many Massachusetts registries have made their records available online, enabling one-stop shopping for a potential thief who stumbles across your name, address, and Social Security number.[3] Earlier this year, the Worcester Telegram and Gazette accidentally delivered copies of its newspaper wrapped in printouts covered with the names and credit card numbers of as many as 240,000 newspaper subscribers.

According to the Privacy Rights Clearinghouse, in 2005 there were over a hundred incidents in which large amounts of information were lost or stolen from major financial companies, data brokers, and federal agencies. Most companies will notify potential victims when a loss of information occurs, but most states do not yet require such notification.

HOW CAN YOU AVOID ID THEFT?

Many ID theft victims never learn how their personal information was compromised. A survey conducted by Javelin Strategy and Research in conjunction with the Better Business Bureau found that where the source could be identified, the loss or theft of a credit card, wallet, or checkbook was the most frequent cause.

Ultimately, nothing that you can do will *guarantee* that you won't be a victim. However, you *can* take action to reduce the likelihood of a loss. Here are some ways to reduce the probability of identity theft and to increase your chances of detecting such a theft when it occurs:

1 To an identity thief, your Social Security number is a gift that keeps on giving. Having obtained it, he can open accounts in your name for years, even if you go through the process of getting a new number. You should guard your Social Security number, date of birth, mother's maiden name, and the numbers for all your financial accounts. Documents containing such information should be shredded before leaving your home. Remove your Social Security card from your wallet, and never include it on your checks. Avoid giving your Social Security number to utility companies and other firms that may request it.

2 Minimize your chances of a loss by keeping only what you really need in your wallet. This includes removing any passwords or PIN numbers that you might keep there. Photocopy everything that remains; then, if your wallet is lost or stolen you'll easily know which credit cards have been lost and what information is at risk.

3 Be sure your mail is secure. Envelopes containing bill payments or checks should never be left for mail pickup at your home; if your mail is easily accessible, consider a locked mailbox. You can suspend the use of paper statements and retrieve your statements online if your mail can't be adequately secured. Many credit card companies allow you to set up e-mail "alerts" to inform you of new statements and transactions.

4 Consider reducing or even eliminating your use of checks. Paper checks don't receive the liability protections given to credit and debit card transactions. Moreover, a check may pass through many hands in the course of a single transaction. If your checking account is compromised, you could spend weeks dealing with bad checks and overdraft charges. When possible, use credit cards and online bill-paying services instead of checks. Federal law limits your fraud liability to $50 for credit cards, and many credit card issuers will waive your liability entirely when fraud is detected. If you can't avoid the use of checks, at least keep your checkbook at home, where the likelihood of loss or theft is reduced.

5 Make sure your credit cards and checks are secure all times. Sadly, a significant amount of identity theft is attributed to family members, coworkers, and others with access to a victim's ID information. Individuals with untreated drug, alcohol, or gambling problems pose the highest risks.

6 Be aware that debit cards don't receive the same fraud protections as credit cards. If you report a stolen debit or ATM card before it is misused, you have no liability; reporting within two days of discovering your loss limits your liability to $50. But if you report a debit card loss after two days, you can be held liable for up to $500. If you fail to report an unauthorized use within 60 days after it is reported in your bank statement, there is no limit to your potential liability.[4]

7 Have each person in your household removed from direct marketing lists by calling the national Do-Not-Call registry at 1-888-382-1222. The major credit bureaus run a service that allows you to opt-out of credit card solicitations by calling 1-888-567-8688.

8 Monitor your credit carefully. Review credit card and bank statements promptly, so that questionable transactions can be identified and corrected quickly. You can request free copies of your credit reports at www.annualcreditreport.com or by calling 877-322-8228. You're entitled to one free report per year from each of the three major credit bureaus (TransUnion, Experian, Equifax). You can make the best use of your free reports by ordering one report

---

[2]"State's online records pose risk" by Joe Light, Boston Globe, June 23, 2005 http://www.boston.com/business/technology/articles/2005/06/23/states_online_records_pose_risk/
(this link may require site registration)

[3]Links to MA registries are available at http://www.sec.state.ma.us/rod/rodidx.htm . If you find your Social Security number in one of these registries, write to the Registrar of Deeds and ask that your information be removed from paper and online documents.

[4]http://www.ftc.gov/bcp/conline/pubs/credit/atmcard.htm

from a different bureau every four months. Look for incorrect addresses or accounts that you don't recognize and alert credit bureaus to such errors.

9 If your accounts offer online access, check regularly for unauthorized transactions. Regular online monitoring has been found to reduce the frequency and severity of identity theft losses.

Signs that MAY indicate that you have been a victim of identity theft:

1. You don't receive credit statements when expected. This may indicate that a thief has taken control of an account and changed the billing address.
2. Your credit is denied for no apparent reason.
3. You receive calls or correspondence about something you never bought.
4. You receive a credit card you didn't apply for.

WHAT ABOUT CREDIT MONITORING SERVICES?

For most people, the monitoring services offered by the main credit bureaus are probably not worth the cost, because each credit bureau only monitors its own reports. An account irregularity reported by one bureau might not show up on other bureau's report for some time. Also, monitoring services can't *prevent* theft, though they can improve your chances of detecting a theft once it has taken place. If you have *already* been a victim of identity theft, especially in a case where a thief has opened new accounts in your name, you *should* use a monitoring service. You should also seriously consider a monitoring service if you've had your Social Security number compromised. In both instances, you have a higher risk of future problems.

WHAT SHOULD YOU DO IF YOUR IDENTITY IS STOLEN?

Even the strictest vigilance may not keep you from experiencing identity theft, but prompt reporting of a theft can minimize your losses. If you discover that you've been victimized, take the following steps immediately:

1 If you know where the theft took place, file a police report. This documentation could be valuable later.

2 Close any accounts that have been opened or used fraudulently.

3 Contact a major credit bureau and ask for a fraud alert to be placed on your accounts; the bureau must then forward your alert to the other two credit bureaus. A fraud alert advises creditors that you are a victim of ID theft and directs them to contact you by phone before opening new accounts in your name (there is no *guarantee* that this directive will be followed, but in my experience, it has worked). An alert can be placed on your credit reports for up to seven years if you are a fraud victim.

4 File a report with the Federal Trade Commission, which can sometimes help you with resolving problems that arise as a result of ID theft.

Finally, here are some more resources available to assist you in preventing or dealing with ID fraud:

FEDERAL TRADE COMMISSION
www.consumer.gov/idtheft/
877-438-4338

CALL FOR ACTION
www.callforaction.org
866-IDHOTLINE

https://www.truecredit.com/help/learnCenter/identityTheft/overview.jsp
http://www.privacyrights.org/identity.htm
http://www.idtheftcenter.org/index.shtml
www.fightidentitytheft.com

CREDIT REPORTING AGENCIES:

TransUnion	Experian	Equifax
800-888-4213	888-397-3742	800-685-1111

FISHER FINANCIAL STRATEGIES

Thomas A. Fisher

Suite 1800
245 First Street
Cambridge, MA 02139

Phone: 617-444-8555
Fax: 866-312-5605

Tom@FFScambridge.com
www.FFScambridge.com