PUBLISHER'S NOTE:

Anne A Rutherford, Financial Advisor at Morgan Stanley Smith Barney LLC, supplied the following article to help Cape Women protect themselves from identity theft.

Protecting Yourself from Identity Theft

by Morgan Stanley Smith Barney LLC.

No one can doubt the immeasurable benefits of the information revolution. Today, thanks to e-mail and the Internet, many of us are more productive, informed and connected than ever before. Unfortunately, as a result, we are also more vulnerable.

The statistics are startling. According to a 2006 survey conducted by The Better Business Bureau and Javelin Strategy and Research, nearly nine million people were victims of identity theft, costing a total of approximately $56.6 billion.

Understanding Identity Theft

Identity theft can take many forms. It typically occurs when someone uses your name and confidential information, including your social security number, date of birth and mother's maiden name, to do something you didn't authorize.

Perpetrators may take out a loan, use your credit card, open a new credit card in your name or withdraw money from your account.

A thief can obtain information about you by stealing your wallet, breaking into your car or home, going through your trash or illegally taking mail out of your mailbox.

More sophisticated techniques include hacking into databases and websites, sending out fake e-mails (called "phishing"), buying website addresses similar to those of financial institutions and creating computer "spyware" programs that record your keystrokes.

Information has also been stolen from computers, from data mistakenly posted on public websites and illegally copied when credit or debit cards are swiped to pay for a purchase.

Vigilance Pays

Charges or withdrawals you don't recognize on statements from your credit card, bank or brokerage firm, failure to receive a new credit card upon expiration or a check that a payee didn't receive, all point to the possibility that someone may have accessed your account without your knowledge.

How can you protect your personal information? You can reduce your vulnerability by being vigilant about protecting your personal information, monitoring your financial transactions, using updated computer technology and protecting your credit.

Here are some specific steps you may wish to consider:

Maintain Your Privacy

- Before giving out your date of birth, social security number or driver's license number, ask why the information is needed.
- Use a good shredder to dispose of anything containing your personal information: account statements, credit card solicitations, checks (both canceled and unused), paycheck stubs and medical records.
- Include only the last four digits of your credit card account on checks when sending a payment to your credit card provider.
- If mail containing a canceled check or financial information has been tampered with, you may want to close the account and open a new one.

Monitor Financial Communications

- If someone contacts you by phone, letter or e-mail, claiming to be from your financial institution and informs you of

unusual account activity or asks questions to verify your identity, don't provide any information.

Call the financial institution's main number (listed on your account statement or on the back of your card) to ensure that you're speaking with an authorized representative and report the incident. Be just as circumspect with an e-mail from a financial institution—if you hit "Reply" or go to a website listed in an e-mail, you risk falling into a trap.

- Scrutinize every account statement you receive and make sure you can identify all the transactions. Some thieves will put small charges on your card (some under $1) to see if you catch on before they start making larger purchases.
- Mail and paper are still currently the most common path to identity theft. If properly used, electronic receipt of statements and electronic bill payment can be safer than some paper-based transactions.

Use Updated Computer Technology

- If you're using a computer at home, keep your operating system up to date, set up a firewall and keep your virus protection and spyware detection programs current. If your computer has a feature for Internet use that notifies you if a form you're submitting is being redirected, be sure that feature is activated.
- When conducting online transactions, look for "https" at the beginning of a website's address—the "s" indicates that the information was transmitted in encrypted fashion from a secure site.

Safeguard Your Credit Information

- Consider using one credit card that has a low limit for online purchases.
- Keep copies of your credit cards in a safe place in your house, and carry only the cards you need.
- Cancel and then cut up credit cards you don't use.
- Take advantage of the free credit report you can get from Equifax, Experian and TransUnion, the three major credit bureaus.
- You can call 1-877-322-8228 or go to www.annualcreditreport.com.Review the accounts in your name - if you don't recognize them, contact the credit bureaus immediately.

How to Respond

Unfortunately, even the most cautious of consumers can still be victimized by identity theft. If it happens to you, here are five steps that can help:

1. Call your financial institution immediately and close the compromised account. Ask what they recommend you do next.
2. File a complaint with the Federal Trade Commission: http://www.consumer.gov/idtheft, 1-877-438-4338.
3. Contact the Social Security Administration: http://www.ssa.gov/oig/public_fraud_reporting/index.htm, which maintains a fraud hotline, 1-800-269-0271.
4. Contact the fraud division of one of the three main credit bureaus to consider having a fraud alert put on your file. The credit bureau will then notify the other two bureaus of the fraud.
5. The free 90-day security alert informs creditors that they must contact you before opening a new account or making changes to your existing account.
6. You can file a police report and submit a copy to the financial institution affected by the fraud as proof of the crime.

In working with credit card companies, banks, credit bureaus and law enforcement agencies, the time it takes to recover from identity theft can be extensive.

The Javelin/Better Business Survey also found that victims of identity theft spend a high of 40 hours each recovering from the crime. Protecting your information to begin with is certainly the most cost- and time-effective strategy.

MorganStanley
SmithBarney

Anne A Rutherford
Financial Advisor
Morgan Stanley Smith Barney

352 Main Street
Falmouth, MA
1-508-457-3367
anne.a.rutherford@mssb.com

Equifax 1-800-525-6285 www.equifax.com

Experian 1-888-397-3742 www.experian.com

TransUnion 1-800-680-72890 www.transunion.com