

## BBB Tips Detecting Identity Theft: The Quicker, The Better

According to the 2005 Identity Fraud Survey Report, released by the Better Business Bureau and Javelin Strategy & Research, one in 23 adults can expect to be victimized by identity thieves, generating more than \$50 billion in losses.

Prevention, however, is but one way to combat this white collar crime. Early detection is also key. The survey research shows that more than half (54%) of the victims of identity fraud discovered on their own that they were victims; in other words, they self-detected the crime. And, a significant portion (44%) of those who self-detected the fact they had been victimized, did so through monitoring of their accounts, either through paper statements or electronic means (the Internet, ATMs or the telephone). Finally, those who used electronic means discovered the loss sooner and experienced a dramatically lower loss.

In light of the findings, the BBB recommends that consumers and businesses consider the following steps, which would prove helpful should their personal identity become compromised:

- **Monitor Your Account Balances And Activity At Least Weekly.** For existing account fraud (that is, identity fraud committed against your own accounts), your best defense is to catch the fraud as early as possible. Electronic access to your account -- either through the Internet, your telephone or an ATM -- allows you to monitor your account activity on an ongoing basis, rather than waiting for a paper statement to be mailed to you. The survey shows that the average fraud amount of those who caught their fraud as a result of monitoring paper statements was roughly \$4,500, while the average amount was \$550 for those who monitored their accounts using electronic means. Higher loss amounts also prove more difficult to resolve.
- **Use e-mail-based account "alerts" to monitor transfers, payments, low balances and withdrawals.** Many financial service companies offer free "alerts" to let you know when your account balances have dropped below pre-set limits or when transfers, payments or withdrawals have been made from your account. If you are not monitoring your account on a daily basis, you can take advantage of these "alert" services. If you spot activity that you believe is not yours, contact your financial institution immediately.
- **If you do not have access to online accounts, review paper bank and credit card statements monthly and monitor your billing cycles for missing bills or statements.** While electronic means will permit you to review your statements more frequently, thereby increasing the chances of catching a fraud before it does extensive damage, you can still limit the damage by carefully checking your paper statements every month. Make sure you know when in the monthly cycle you are scheduled to receive your statements. If you notice that one is missing, that could be a sign that someone may have stolen a statement (and, perhaps your cancelled checks) from your mailbox.
- **Monitor your credit report at least annually.** New account fraud (when someone uses your identity to open a new account in your name) is more difficult to detect. There's no way, of course, to monitor accounts that have been opened in your name without your knowledge. That's where your credit report is so important. When someone tries to open an account in your name, the credit grantor will check your credit report before granting credit. If credit is granted, the new account will subsequently show up on your credit report.

All Americans are entitled to receive a free copy of their credit report once each year. In Georgia, you are allowed two free copies of your credit report from the three major credit bureaus each year. The three major credit reporting agencies (Equifax, Experian and TransUnion) have created a single Web site ([www.annualcreditreport.com](http://www.annualcreditreport.com)) where you can go to get more information on how to request your report. For a fee, the reporting agencies also offer more frequent monitoring services to alert you when your report is accessed and when other events take place.

- **Consider Moving to Online Statements and Bills and Paying Bills Online Whenever Possible.** More and more people now bank, pay bills and receive statements online through secure Internet sites. If you decide to join those ranks, consider eliminating paper bills, checks and statements and carefully safeguard any paper copies that you do choose to print out. Also, consider placing a password protection on your computer and your sensitive files (such as your online banking file); ensure that your computer has a firewall to protect from Internet attacks; install and regularly update anti-virus/anti-spyware software on your system; and, keep the security features of your computer's operating system current.