

# American Heritage Protective Services

## “Protect Against Identity Theft”

*During the course of a normal day you may write a check at the grocery store, charge tickets to a sporting event, call home on your cell phone, order new checks for your checking account, or maybe even apply for a new credit card. Chances are that you don't give any of these everyday transactions a second thought, but someone else may.*

In the 1990's a new variety of crook called an identity thief appeared. This thief's stock in trade is your transactions. Each transaction requires you to share personal information: your bank and credit card account numbers, your income, your Social Security Number (SSN); and your name, address and phone number. An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all too common example is when an identity thief uses your personal information to open a credit card account in your name.

It is estimated that in 2001 upwards of 750,000 people had their identities stolen and are currently trying to recover from their losses. Although data from last year is still being compiled, it is believed that the number of identity theft victims in the nation will easily top the 1 million mark. In a single incident in 2002, the State of California had its entire employee database, which included more than 260,000 workers, exposed to a hacker. Despite the best of efforts to manage the flow of personal information or to keep it private, skilled identity thieves may use a variety of methods – both low & high tech – to gain access to data. Many consumers feel that they may be safe from identity theft because

they don't make credit card purchases over the Internet or the phone. This is a complete misconception since virtually everyone over 18 is part of the nation's credit reporting system, which therefore makes them susceptible to identity theft. Recently, an employee of a small Long Island, New York communications company was arrested after he allegedly masterminded a ring that cost consumers over \$2.7 million. In this case the alleged suspect had sold the credit reports of more than 30,000 customers of the communications company. These reports included information such as bank accounts, credit card numbers, even former and current addresses. After their personal information was sold to identity thieves, victims discovered that loans had been taken out in their names and that they owed money on cars, boats, and in some cases, houses. When a consumer finds out their personal data has been leaked, the waiting game begins. They should order credit reports regularly and simply monitor if their bank accounts become the victim of unplanned withdrawals, if car loans are taken out in their names, if their homes are mortgaged and whether equity is stolen right out from under their roofs.

The healthcare field can be particularly vulnerable with regard to identity theft. Healthcare administrators must be certain that not only are safeguards in place, which will hopefully discourage employees from considering becoming involved in schemes to use current or former patient information in identity theft scams, but also to implement protective measures that can stop a potential identity thief from obtaining fraudulent healthcare services.

## Important Tips:

While identity theft can't be prevented entirely, the risk can be minimized. By managing personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft by:

- *Determining how personal information will be used and whether it will be shared with anyone before you reveal it.*
- *Paying attention to billing cycles, and following up with creditors if your bills don't arrive on time.*
- *Guard your mail from possible theft by depositing outgoing mail at the Post Office and promptly removing mail from your mailbox.*
- *Putting passwords on your credit card and bank accounts and avoiding the use of easily available information for PIN numbers.*
- *Limiting the identification information and number of credit cards you carry to what you actually need.*
- *Not giving out personal information on the phone, through the mail or the Internet unless you initiated the contact or you know who you're dealing with.*
- *Keeping items with personal information in a safe place, as well as tearing up or shredding charge receipts, credit applications, bank statements, or expired charge cards.*
- *Determining who has access to your personal information at work and verifying that these records are maintained in a safe location.*
- *Providing your Social Security Number only when absolutely necessary.*
- *Not carrying your Social Security Card with you and keeping it in a safe, secure location.*
- *Ordering a copy of your credit report at least annually.*

The US Congress has asked the Federal Trade Commission (FTC) to provide information to consumers about identity theft and to take complaints from those whose have been stolen. If you, or someone you know may have been the victim of an identity theft, call the FTC's Identity Theft Hotline toll free at 1-877-ID-THEFT (438-4338). The FTC puts this information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies and private entities, including any companies about which a victim may complain.

In addition the FTC has developed an ID Theft Affidavit – a form that can be used to alert companies where a new account was opened in a victims name. Companies can then investigate the fraud and decide the outcome of these claims. A list of some of the companies and organizations that accept or endorse the ID Theft Affidavit can be found at: <http://www.consumer.gov/idtheft>. The FTC working in conjunction with other government agencies has produced this report to help victims and potential victims guard against and recover from identity theft.



Contributed by:  
**Stephen J. Pollak**  
*Executive Vice President*

Prior to his current position with American Heritage, Mr. Pollak served 24 years with the Mokena Police Department, the last 14 years as Chief of Police. He holds a Master of Science degree in Criminal Justice, a Bachelor of Science degree in Education, and is a graduate of the 162<sup>nd</sup> Session of the FBI National Academy. He and his wife Karen of 26 years are the parents of three daughters. In his spare time he enjoys golfing, toy collecting, reading, and playing volleyball.

### AHPS Can Help

For assistance in the creation of a crisis plan for your business call American Heritage Protective Services toll free at 866-830-1800. Visit our website at [www.ahpservices.com](http://www.ahpservices.com).