Identity Theft

Identity theft is said by many to be one of the fastest growing crimes today. The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year. Thieves use the identity of others to obtain credit cards, take out loans, charge goods and services to credit cards, obtain medical care, rent apartments, obtain utility services, etc., all in the name of the victim. Victims often do not become aware of the misuse of their identity until they seek to obtain a loan themselves and learn that their credit record contains one or more unpaid accounts of which they were not previously aware. It may take years to completely restore the victim's credit.

Typically, the focal points for identity theft are the victim's Social Security number (SSN), credit card numbers, and, increasingly, medical insurance identification numbers. In some cases, identity thieves obtain these numbers by going through the victim's trash. For those who know where to look, these numbers are for sale on the Internet. Others call their victims to request these numbers for some official-sounding purpose using telephone systems that cause their calls to falsely appear on the victim's caller ID screen as originating from the victim's bank, doctor's office, medical insurance company, some federal agency, etc.

Still others use official-looking e-mail said to be from an individual's bank or credit union threatening to close his/her account or "requiring" the victim to re-set a password in order to re-activate an account that has been frozen based on too many failed log-in attempts. The e-mail provides a convenient and official appearing link to click to take care of the problem. That link takes the victim to what appears to be an authentic website where his/her user name and password are captured by the thieves, who immediately log in to the victim's account on the real website and transfer out all the funds.

Simple steps to reduce the likelihood of becoming a victim of identity theft include shredding credit card bills, medical insurance explanations of benefits, and other documents containing personal information that can be used by imposters to set up accounts and obtain goods and services in an individual's name. Credit card bills should be reviewed carefully to detect small charges sometimes made by identity thieves in anticipation that they will not be noticed. If a credit card bill fails to arrive on time, the account holder should consider the possibility that an identity thief has filed a change of address on the account as a prelude to a major spending spree using the account holder's credit.

Nationwide consumer credit records are maintained by TransUnion, Equifax, and Experian ("the Big Three"). "Credit watch" services are available from the Big Three and others. These services will provide information as to when a credit record maintained by these three companies changes due to a new account being opened or an existing account balance changing by a specified percentage or amount. However, many doubt the value of these services since they are frequently weeks, if not months, behind in posting information. Everyone is entitled to one free credit report per year from each of the Big Three. By staggering requests at four-month intervals, one can approximate the services of many of the credit watch companies.

It is also possible to impose a "freeze"on one's credit report. Under a freeze, potential creditors are denied access to the report unless the freeze is lifted temporarily or permanently. Since most creditors will need to view a credit file before opening a new account, they may not extend the credit if they cannot see the file. Almost all states provide for a freeze by law. Some states require that freezes be imposed without cost to the consumer. Though Alabama does not have such a law, the Big Three will implement a freeze for Alabama residents for a fee. There may be a charge each time the freeze is lifted and reinstated, and potentially inconvenient lead times may be required for the lifting and reinstating of the freeze.

If an individual has reason to believe that he or she has been the victim of identity theft, a fraud alert should first be placed on credit reports. This can be done by contacting any one of the Big Three. Theoretically, an individual only needs to contact one of the three, since each is required to contact the other two to have an alert placed on their versions of the report too. It may be wise, however, to contact each company directly rather than rely on one contacting the other two. A fraud alert warns potential creditors that they must use what the law calls "reasonable policies and procedures" to verify the individual's identity before they issue credit in his/her name. Under the federal Fair Credit Reporting Act, a person may be entitled to two kinds of free fraud alerts: initial and extended. An initial fraud alert is good for 90 days and can be renewed when appropriate.

Once a fraud alert has been filed, the individual is entitled to one free credit report from each of the Big Three. Those reports should be reviewed and any accounts closed that are believed to have been or that may be affected. A complaint may also be filed with local police and/or police in the area where the fraud occurred and with the FTC.

The FTC maintains a website that is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help one deter, detect, and defend against identity theft. The site includes general advice, form letters, report forms, and addresses and telephone numbers that will be of assistance in dealing with identity theft. That site is found at http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html