Identity Theft - Part 1

Part 1 is a brief explanation of ID Theft and its consequences. Please see Part 2 for information on what can be done to prevent it.

ID theft is another form of fraud that has been around for as long as there have been dishonest people. It is a high-profile problem because technology has created many more opportunities for this crime. Credit cards, funds transfer cards, ATMs, slipshod business practices and the Internet have all combined to make identity theft a major problem for individuals and businesses.

ID theft describes any dishonest and unauthorized use of private information. In the past, the term rightfully described forgery or passing oneself off as another person to trick someone out of money and/or property. Today, it refers to an unauthorized party who secures goods, services, or other financial benefits by the fraudulent use of another person's confidential information.

The favorite piece of information is a social security number. This information has routinely been used for gaining access to other private information such as driver's history, credit information, bank accounts, loan information, credit cards, occupational history, military records, mortgage information, investment accounts and so on. Having this critical bit of information can allow a criminal to use another party's accounts, secure loans, charge a host of goods or services; the list is only limited by the criminal's resources and imagination.

A complication of ID Theft is that it is a by-product of modern commercial life. Lenders, retailers, supermarkets, gas stations, airlines, travel clubs and everyone else have elevated charge accounts into the premiere way to do business, either live or electronically. This "ease" comes at great cost. As naïve as it sounds, business still operates on the assumption that everyone is honest. Few businesses have adequate safeguards to protect the information they collect on customers. Many businesses commonly mail out charge cards and other solicitations that include private account information. It is common for electronic transactions to be transmitted through wireless networks and thieves are now able to intercept such data. Further, since businesses are often embarrassed that information has been stolen or compromised by hackers, many businesses keep such invasions secret or substantially delay reporting incidents to authorities and to their customers.

In light of business practices and attitudes, it's basically up to the individual consumer to guard against ID theft. See Part 2 for tips on guarding against it.
