HOW IDENTITY THEFT OCCURS

I first was notified that someone had used my Social Security number for their taxes in February 2004. I also found out that this person opened a checking account, cable and utility accounts, and a cell phone account in my name. I'm still trying to clear up everything and just received my income tax refund after waiting four to five months. Trying to work and get all this cleared up is very stressful.

From a consumer's complaint to the FTC, July 9, 2004

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods to gain access to your data.

HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION:

- They get information from businesses or other institutions by:
  - stealing records or information while they're on the job
  - bribing an employee who has access to these records
  - hacking these records
  - conning information out of employees

- They may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.

- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."

- They may get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.

- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.

- They may steal your wallet or purse.

- They may steal personal information they find in your home.

- They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or "pretexting" by phone.

HOW IDENTITY THIEVES USE YOUR PERSONAL INFORMATION:

- They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.

- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.

- They may establish phone or wireless service in your name.

- They may open a bank account in your name and write bad checks on that account.

- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.

- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

- They may buy a car by taking out an auto loan in your name.

- They may get identification such as a driver's license issued with their picture, in your name.

- They may get a job or file fraudulent tax returns in your name.

- They may give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

IF YOUR PERSONAL INFORMATION HAS BEEN LOST OR STOLEN

If you've lost personal information or identification, or if it has been stolen from you, taking certain steps quickly can minimize the potential for identity theft.

- **Financial accounts:** Close accounts, like credit cards and bank accounts, immediately. When you open new accounts, place passwords on them. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

- **Social Security number:** Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports. An alert can help stop someone from opening new credit accounts in your name. For consumer reporting company contact information, see page 5. For more information about fraud alerts, see page 6.

- **Driver's license/other government-issued identification:** Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you've taken these precautions, watch for signs that your information is being misused. See **Staying Alert**, page 27.

If your information has been misused, file a report about the theft with the police, and file a complaint with the Federal Trade Commission, as well. If another crime was committed – for example, if your purse or wallet was stolen or your house or car was broken into – report it to the police immediately.