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, either low-or-hi-tech, to gain access to your personal data.

How Identity Thieves *GET* Your Personal Information

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information.
- They complete a "change of address form' to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as 'dumpster diving.'
- They fraudulently obtain your credit card report by posing as a landlord, employer or someone else who may have a legitimate need for, and legal right to the information.
- They find personal information in your home.
- They find personal information you share on the internet.
- They scam you, often through fraudulent email or 'spooled websites' and even over the phone. They pose as legitimate companies or government agencies you do business with. Motivated scammers ask for your financial information, such as your social security number, credit card and debit card numbers, mother's maiden name, passwords, PINs, and other information. Known as phishing, pronounced 'fishing,' this is the latest ID theft scam.
- They get your information from the workplace in a practice known as 'business record theft' by stealing files out of offices where you're a customer, employee, patient, or student; bribing an employee who has access to your files; or hacking into your electronic files.

How Identity Thieves *USE* Your Personal Information

- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because the bills are being sent to the new address, it may take some time before you realize there's a problem.
- They open a new credit card account using your name, date of birth, and social security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They establish a phone or wireless service in your name.
- They establish a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards and drain your bank account.
- They buy cars by taking out auto loans in your name.
- They give your name to the police during an arrest. If they're released from police custody, but don't show up to their court date, an arrest warrant is issued to your name.

Take These Steps to *Minimize* Your Risk

- Order a free copy of your credit report from each of the three major credit bureaus once a year, by going to www.annualcreditreport.com.
- Place Passwords on your credit cards, bank, and phone accounts.
- Never give personal or financial information over the phone if you did not initiate the call.
- Never respond to an email requesting personal or financial information, even though it's looks like it's from a legitimate organization that you do business with and even if the request sounds urgent. Alert the organization identified in the suspect email by using a phone number that you know is legitimate.
- Secure personal information in your home, especially if you have roommates, employ outside help, or are having service work done on your home—even if you think you can trust them.
- Pay attention to billing cycles – if you do not receive a credit card bill on time, call your creditor.
- Tear up or shred junk mail before throwing it away, especially credit card offers.
- Never leave out-going mail in your mail box. Always use a post office collection box.
- Never write your personal identification numbers on the back of your credit or ATM cards.
- When leaving a cash register after a purchase or an ATM, always take your receipt and look at your credit card or debit card to be sure you received your own card back.

Useful contact information:

The Federal Trade Commission website is www.consumer.gov/idtheft or call 877-438-4338 for their Identity theft hotline.

"Do Not Call" list: www.ftc.gov/donotcall.

Internet Crime Complaint Center: www.ifccfbi.gov - A partnership between the FBI and the National White Collar Crime Center. Contact if you think you have received a phishing email or have been directed to a phishy-looking website.

If you think you have been fooled (phished) into giving someone personal or financial information through an email or over the phone, go to www.ftc.gov or call 877-382-4357 to file a complaint.

To receive a free annual credit report, go to: www.annualcreditreport.com.

Credit Bureaus

Equifax – www.equifax.com
To order your report, call: 800-685-1111
To report fraud, call: 800-525-6285
TDD 800-255-0056 and write:
PO Box 740241, Atlanta, GA 30374-0241

Experian – www.experian.com
To order your report, call: 888-EXPERIAN (397-3742)
To report fraud, call: 888-EXPERIAN (397-3742)
TDD 800-972-0322 and write:
PO Box 9532, Allen, TX 75013

TransUnion – www.transunion.com
To order your report, call: 800-888-4213
To report fraud, call: 800-680-7289
TDD 877-553-7803; fax: 714-447-6034; email:
fvad@transunion.com or write: Fraud Victim Assistance Department,
PO Box 6790, Fullerton, CA 92634-6790