

Preventing Identity Theft:

“Do’s and Don’ts”

DO:

Protect your incoming and outgoing mail. Remove your mail from the box as soon as possible. If you believe that mail containing personal or financial information was opened or altered, notify the sender and stay alert for any suspicious activities, such as phone calls to verify your credit card numbers, loans, or bank accounts. If you are expecting a new or renewed credit card or other financial document by a certain date, watch the mail to be certain it arrives, and pursue the matter if it fails to arrive.

Shred or completely tear up any discarded paperwork that contains personal identifiers or financial information, including pre-approved credit card applications. If a vendor uses carbon copies for credit card bills, ask for and destroy the carbons. You can lessen your risk even further by discarding destroyed documents in separate garbage cans.

Be aware of where your personal identification is kept and who has access to it. Protect your wallet and purse and never leave them unattended.

Closely review your bills, including utility bills and bank statements, to ensure that all balances and receipts match and no activity is unaccounted for. If you do not get a statement or bill, find out why it is missing.

We also advise you to install software on your computer, available at most computer stores, that encrypts information you send in an e-mail. You can also ask your financial institution to add security to your accounts, such as special passwords.

Stop pre-approved credit offers by calling all three credit reporting bureaus and opting out of the programs. By opting out, you receive fewer pre-approved loans and credit applications.

DON'T:

Do not give out personal information in response to unsolicited offers by phone, mail, Internet, or in person. Criminals may pose as legitimate business people, charity workers, or law enforcement officers to gain your trust.

Do not use your Social Security number unless you have to, including on your driver’s license and checks. The Illinois Secretary of State allows drivers the option of not having their Social Security number on the driver’s license.

Do not fill out warranty cards for items you purchase or enter sweepstakes. Such information is often sold to others as a marketing tool.

Personal identifiers, account numbers, and other private information should not be provided to anyone, unless you know the information will be secure.

If you follow these steps, you will reduce your risk of being a victim of an identity theft, but you can not completely eliminate the risk. Your goal should be to reduce other people’s access to your information, so you should know what people and companies do with the information you give them. Keep these facts in mind:

- Know the person or company to whom you give information
- Ask what the person or company will do with the information
- Err on the side of caution—keep an eye on your financial picture, so if irregularities occur you will recognize them.
- Remember: Although you may not have to pay