

## ***What is identity theft?***

Identity theft occurs when someone uses someone else's identifying information without that person's consent, for the purpose of profiting unlawfully.

## ***What are some typical examples of identity theft?***

Identity theft occurs in many ways. Someone may steal identifying information of a U.S. citizen in order to sell it to someone else who is in the country illegally and who needs ID in order to work. Identity theft can occur when someone who receives Social Security retirement checks dies—and the person's family or caregiver intentionally never tells the Social Security Administration to stop sending monthly checks. Some identity thieves "take over" one of your credit cards and run up a huge bill; or find a way to write checks on your bank account; or use your credit card as proof of "creditworthiness" in opening more credit card accounts in your name, or borrowing large amounts of money under your name. In some communities, identity thieves have pretended to operate clinics for the elderly so that they can get Medicare and Social Security numbers to use in sending phony medical bills to the government for reimbursement. In a similar scheme, "doctors" and "nurses" bring a mobile "blood pressure unit" to neighbor-

hoods where they offer free services in exchange for Medicare identifying information. Some identity thieves use others' identifying information to draw unemployment benefits without the person's ever knowing the benefits were used.

In short, the types of identity theft seem to have no limit—unless the potential victims of this crime work hard to prevent it!

## ***Who is likely to be an identity thief?***

The thief can be anyone who has access to your unique identifying information—your Social Security or Medicare number, your bank account number, your credit card information. That means that the thief could be someone who works at your corner store, someone in a doctor's office, someone who grabs mail from your home mailbox, someone who "hacks" into supposedly secure computer data bases to obtain credit card information or other unique identifying information. Not even the national credit reporting agencies are immune from phony "landlords" or "merchants" who call in to get credit information about someone they claim is a potential tenant or customer.

The government estimates that about 30 per cent of identity thieves are small-time operators—care givers, family members, pickpockets, people who root through your trash looking

for a quick way to make some money. About 70 per cent of identity-theft crime is the work of sophisticated criminal syndicates.

### ***Whom do identity thieves target?***

According to the FBI, identity thieves target older persons nine times out of ten. Older people have more assets than younger people, and often have better credit.

In addition, older people are more likely to have landline telephones—making it easy for thieves to learn their addresses and to call them with get-rich-quick “offers” or requests for donations to a fake charity, just to learn identifying information that can be used in financial crimes.

### ***Why has identity theft become so common?***

The FBI says that the average stolen identity typically gets sold to new crooks several times—and is worth about \$30,000 on the black market. That is a lot of money—and a lot of incentive to thieves.

Changes in technology have helped make identity theft easy and profitable, too. Computer “hackers” steal personal information from many sources—giant companies (including insurance and credit card companies and banks) and even from the state and federal government.

Many identity thieves use the internet to persuade innocent people to turn over information voluntarily—by pretending in an email message to be the Social Security Administration, the Center for Medicare and Medicaid Services, the IRS, your bank, or your credit card company. Often these messages claim that your personal information has been lost or stolen, and that the agency or business needs to “update” your private information. They tell you to submit that information to a website that looks like—but isn’t—the official agency they claim to be.

It is important to remember that real government agencies and legitimate businesses *never* ask either by email or on the phone for this kind of information.

### ***How would I know if my identity has been stolen?***

You could find out in several ways: your checks suddenly bounce; your credit card bill suddenly goes sky-high; you hear from a collection agency or business demanding payment for something you never bought. Although your credit has always been good, you may get turned down for a mortgage or a car loan. You may apply for unemployment benefits only to be told that “you” have already used up your benefits. A

few people have found out their identity was stolen when a police officer knocked on their doors—ready to arrest them for a crime committed by someone who has been using their name!

### ***What can I do to avoid becoming a victim of identity theft?***

There are many things you can do to minimize the chance that you will fall prey to an identity thief:

- use a secure mailbox—either a locked one at your home or a post office box
- use a shredder to get rid of all identifying information that you receive in the mail or that appears on medical bills and credit card and other receipts. If you can't afford a shredder, tear off all identifying information from your mail and from credit card receipts, medical billings, and other sources of identifying information, and “cook” that information in a pot of boiling soapy water until it dissolves.
- If you have a landline phone, put your name on the national “do not call” list. Once your name is on the list, legitimate businesses will no longer call you. Unfortunately, that means that the odds are very high anyone who does call you is a

- crook. Remember that the “do not call” list doesn't limit political campaigns or charities from calling you—and that it is impossible to tell a real charity from a fake charity on the phone. It is a good idea to decide which charities will get your donations, and not to succumb to telephone requests for contributions. The amount the caller asks for may be small, but the damage that person can do to your credit after getting your personal information can be very serious. Remember also that your registration on the do-not-call list ends after five years. You must renew your registration to keep callers away.
- Lock checkbooks, passports, credit card information, bank statements, your Social Security and Medicare cards, and anything else with identifying information on it, in a safe place, where caregivers and others cannot get them.
  - Don't carry your Social Security or Medicare or Medicaid card with you.
  - Ask doctors and others to remove the first five digits of your Social Security number from their records.
  - Read your bills, bank statements, credit card statements, and Medicare Explanation of Benefits statements as soon as

you get them, to see if there is unusual activity or a medical procedure you don't recognize.

- If you have a choice, pay for things with cash. If you must use a card to pay, use a credit card rather than a debit card. If there is unauthorized use of your credit card, your liability is limited to \$50. The only limit to the amount of money an identity thief can take from your bank account is the amount of money that is in the account.
- Don't send any identifying information over the internet unless you have initiated the contact and the site is a "secure" one.
- Ask for a copy of your credit report annually from the three main credit reporting agencies. You are entitled to a free copy once each year; if you believe you are the victim of identity theft you are entitled to a free copy when you report the theft.
- Avoid entering contests or sweepstakes and answering surveys that come in the mail or that you see online. The more contacts you make online, the more likely it is that someone will be able to hack into your information somewhere.

***What do I do if I find out I am a victim of identity theft?***

There are several things you should do, and the sooner you do them the better:

- contact the police to make a report, and get a copy of the report
- close any accounts that you think someone has accessed or set up fraudulently
- send a notice about the identity theft to the three national credit reporting agencies, enclosing a copy of the police report
- send a copy of this notice and the police report to the Federal Trade Commission
- Ask the credit reporting agencies to put a 90-day "fraud alert" **on your account. Your creditors should then call you before charging your account, but they don't have to and some charge anyway.**
- **credit bureaux can conduct "credit monitoring", for a monthly fee. If they notice an unusual charge, they will notify you—after the charge has been made.**
- **credit bureaux can impose a "credit freeze" for a monthly fee. With a credit freeze, the only creditors who can look at your account are those whom you have given your identity code number. If you want to use a new creditor, you must "thaw" your frozen account to**

allow the creditor to see your records. There is a charge for the thaw. It can take 3-5 days for a thaw to take effect. Then, after the new creditor has reviewed your credit information, you must freeze the account again or it is open to all.

*Caution!* A common consumer scam involves offers from private companies to let people look at their “free” credit reports for a fee, and then monitor their accounts for them for another fee. Make sure that when you sign up for your annual free credit report that you do not sign up for anything else that you don’t intend to pay for.