

STOP,
THIEF!
AND GIVE
ME BACK
MY NAME!



On average, over 1,000 persons a day fall victim to identity theft in the United States. What is identity theft? It's when a thief gets his hands on your personal information and uses it to set up credit in your

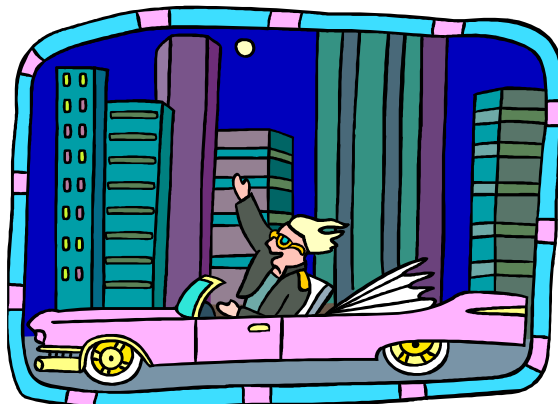


name. Usually, victims don't even know that they've been had until they

order a copy of their credit report, or until they are unable to make a credit purchase because they've seemingly reached their credit limit prematurely.

Look up "identity fraud" on the internet and you'll find an abundance of stories of victims who have lived through the nightmare of having their credit ruined by these thieves.

One couple, John and Mary Stevens, received a call one day and were asked why they were delinquent on payments for a \$27,000 Jeep Cherokee,



which was bought new in Dallas the previous year. Some-

one had purchased the Jeep, four more cars, and 28 other items—worth \$113,000 in all—in their names. How can this happen?

In one case a woman used her credit card to pay a restaurant bill.

Twenty minutes later, the waiter used her card number to charge \$20 calling a sex chat line.



According to Bob Kuykendall, a fraud program manager of the U.S. Postal Inspection Service, "Every identifying number you possess—Social Security, credit card, driver's license, telephone—is a key that unlocks some storage of money or goods. So if you throw away your credit card receipt and I get it and use the number on it, I'm not becoming *you*, but to Visa, I've become your *account*."

One major problem, according to the experts, is that the Social Security number (SSN), which was originally meant only for benefit and tax purposes, has become the universal identifier. It is used as ID by

the military, many health insurance companies, and as drivers' license numbers in many states as well as in billions of commercial transactions.

And it's easy for a thief to hijack your SSN. In addition to stealing your wallet, a thief may take mail from your box, going through your trash for discarded receipts and bills (known as



dumpster diving in the trade) or asking for it over the phone on some pretext.

Other means of getting your personal information include completing a change of address form to divert mail to another location, fraudulently obtaining a credit report by posing as a landlord, employer, or someone else who may have a legitimate need for—and a legal right to—the information, getting personnel or business records at work, finding personal information in your home, using personal information you share on the internet, or purchasing personal data from “inside” sources—for example, an identity thief may pay a store employee for information about

you that appears on an application for goods, services, or credit cards.

Once he has your SSN, the thief may apply for a credit card in your name, asking that it be sent to a different address than yours, and uses it for multiple purchases. A couple of months later, the credit card



company, or its debt collection agency, presses you for a payment. Although you may not have to repay the debt,

it can be a nightmare trying to clear up your tarnished credit record. That means trying to get a police report and copy of the fraudulent contract; then using them to clear the fraud from your credit report, which is held by a credit bureau. Each step can be an epic hassle, and may take both a lot of time and money.

In the Stevens' case, it took three years of paper work and \$6,000 in legal fees. In



the meantime, they were denied a loan to build a vacation

home, forced to pay cash for a new heating and cooling system, harassed by debt collec-



tors, and suffered the humiliation of having their home put under surveillance by investigators looking for the missing jeep. Other victims have been denied

jobs, had their drivers' licenses suspended, and have even been jailed for offenses committed by their identity hijackers.

Thieves may call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account before he runs up charges on the account. They may open a new credit card account, using your name,



date of birth, and SSN. Then they use the card and don't pay the bill. They may also establish phone or wireless service in your name. Thieves can open a bank account in your name and write bad checks on your account.

They counterfeit checks or debit cards and drain your bank account.

And then, some of them file for bankruptcy under your name to avoid paying debts they've incurred under your name!



According to the Federal agencies that handle identity theft, police can sometimes be reluctant to investigate these cases because they consider the banks or the stores, who are out of pocket, to be the real victims. The creditors themselves usually write the debt off as a business loss or claim it against insurance and take no further action.

When credit cards are involved, the Fair Credit Billing Act limits the victim's liability for fraud to no more than \$50, and the card issuer often waives that fee. Federal law provides some protection against

fraudulent use of ATM and debit cards, though the victim's liability may depend upon how quickly the fraud is reported. If someone steals your checks and forges your signature, state law protects you. Most states hold the bank responsible for losses from a forged check; however, they also require consumers to take reasonable care of their



account. You may be held responsible for a forgery if it is deter-

mined that you failed to notify the bank in a timely manner that a check was lost or stolen.

In 1998, Congress made identity theft a federal felony by passing the Identity Theft and Assumption Deterrence Act. This act set up an identity theft unit at the Federal Trade Commission (FTC) to help victims. Violations of this law are investigated by the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Social Security Administration's Office of the Inspector General. The U.S. Department of Justice prosecutes Federal ID theft cases. In most instances, a conviction for ID theft carries a maximum penalty of 15 years imprisonment, a fine, and forfeiture of any personal

property used or intended to be used to commit the crime.

Beth Givens, head of the Privacy Rights Clearinghouse in California, a nonprofit group that has helped victims since 1993, says, "last year the credit industry mailed out 3.5 billion preapproved offers of credit to Americans. And without properly verifying the identity of applicants, they're giving out an awful lot of credit cards to imposters."

Now that you've got an idea of the risks involved, how do you protect yourself from identity theft? Although it's nearly impossible to completely eliminate the possibility, you can greatly reduce your risk by fol-



lowing a number of precautions:

- Never carry your SSN in your wallet or diary or printed on checks. Guard your SSN

closely, giving it out only to official authorities or businesses you trust. Some firms will accept another identifier if you ask.

- Check bank and credit statements and report any unfamiliar charges to the card issuers.
- Exercise your right to stop your credit header being sold, which will also stop pre-approved offers of credit. Call the credit bureau's special toll-free line:
1-888-567-8688
- Don't post personal information on the Internet—for example, on genealogical or college reunion sites.
- Make a list of your credit cards, their account numbers, and their phone numbers. If your wallet or purse becomes lost or stolen, call and have them put a freeze on them.
- Report the loss of a check, your wallet, or purse to the bank and to the police as soon as you discover it's missing.



- Be careful about divulging personal information. Try to avoid giving out your SSN, date of birth, or mother's maiden name to someone over the phone or on the Internet when you haven't initiated the transaction.



- Cancel unused credit cards. Cutting them up is not enough.
- Be careful of how you dispose of credit card solicitations, statements, canceled checks, and financial documents. Ideally, shred them.
- Order credit reports at least once a year from one of the credit reporting agencies:

Equifax.....800-525-6285

Experian.....800-301-7195

Trans Union..800-680-7289

Report any accounts you did not apply for.

- Have your name removed from lists sold to companies offering preapproved credit cards by calling one of the

credit agencies listed above.

- Do not allow sales clerks to copy your credit card numbers onto checks for additional information.
- Call your credit card company if your card has expired and you have not received a new one.
- Carry only a few credit cards with you.
- Never write down PINS and passwords: Memorize them. Do not use any part of your SSN, your name, address, or any easy to guess words or sequences.
- Only release your Social Security number when absolutely necessary. If a business requests it for identification, ask to have an alternative number used.
- Install a locked mailbox at your residence.
- Do not leave paid bills in your mailbox for the mail carrier to pick up.
- When you order new checks, do not have them sent to your home mailbox. Pick them up at the bank instead.
- Never include your SSN on personal checks.

When there's a problem...

Exactly what you do to pro-

protect yourself depends on your circumstances and how your identity has been misused. Nevertheless, it is appropriate to take four basic steps in just about every case:

1. Call the fraud departments of all three credit bureaus. Ask them to put a "fraud alert" on your file. That tells creditors to call you before they open any more accounts in your name.
2. Contact the credit grantors involved—for example, the bank or credit card issuers



who opened the fraudulent account or allowed access to your existing account. Close all affected accounts immediately.

3. Contact your local police and ask to file and get a copy of their report. Even if they can't catch the identity thief, having a police report can help you clear your credit records later on.
4. File a complaint with the

Federal Trade Commission.
Call the FTC's Identity Theft
Hotline toll-free or use the



complaint form at
its website (see back cover
for these).

Consumer Alert! **Internet Account Updates?**

If you receive an e-mail request that appears to be from your Internet Service Provider (ISP) stating that your "account information needs to be updated" or that "the credit card you signed up with is invalid or expired and the information needs to be reentered to keep your account active," do not respond without checking with

your ISP first. According to information received by the FTC, this may be a scam.

In light of all of this information, it's probably pretty clear why our office strongly advises people.....

Do not leave your personal belongings in the hallways, cafeteria, Library, student lounge, or in any other unsecured area. If you must leave belongings behind, leave them in a locked locker.

If you have an office, when you're not in it, lock it.

Do not share personal information with persons who may be soliciting this information in exchange for "free" e-mail or any other such excuse.

Immediately report any lost or stolen items (particularly keys—College or personal keys—wallets, or purses) to the Office of Campus Safety.



Federal Trade Commission's
Bureau of Consumer Protection
Washington, D.C.

To report identity theft:

Call toll-free: 1-877-ID-THEFT
(which is 1-877-438-4338)

Write to:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Online:

[Online ID Theft Complaint Form](#)



This booklet was prepared by
Donna Dobbler for

**Finger Lakes
Community College**

Office of Campus Safety
4355 Lakeshore Drive
Canandaigua, NY 14424
716-394-3500, extension 7213