IDENTITY THEFT:

What You Don't Know Can Hurt You

Consumer Alert!

1-888-995-7856 ALLIANCE Credit Counseling

By Edward Tonini, Director of Education.

Each year:
- **10 million incidents**
- **$5 billion in losses**

Are You Next?

By illegally using your personal information, a thief can make charges to your credit card accounts or open new accounts in your name, drain your bank accounts, obtain loans, open utility services, and more.

A Federal Trade Commission survey states that nearly 10 million people - approximately 1 in 30 Americans - become victims of consumer fraud and identity theft each year. The survey reports the annual losses to consumers at $5 billion. (Source: www.ftc.gov/opa/2003/09/idtheft.htm)

What Is Identity Theft?

Identity Theft is the act of someone obtaining your personal information to impersonate you in order to commit a crime. The Federal Trade Commission (FTC) states that "Identity theft occurs when someone possesses or uses your name, address, Social Security number (SSN), bank or credit card account number, or other identifying information without your knowledge with the intent to commit fraud or other crimes." (FTC, *Identity Theft: What's It All About*)

Some Warning Signs

Sometimes, there may not be immediate signals that you have become a victim of identity theft. The Federal Trade Commission, however, lists some warning signs:

- Your monthly credit card and bank statements suddenly stop arriving.
- You are denied credit for no apparent reason.
- You start getting bills from companies you do not recognize.
- Credit collection agencies try to collect on debts that do not belong to you.

(FTC, *Identity Theft: Your Good Name Gone Bad*)

Contents On Back

Protecting Yourself

Although it is impossible to guarantee you will never be a victim of identity fraud, the Federal Trade Commission lists several things you can do to reduce your risk:

- Regularly check your **credit report** for accuracy and report errors.
- Place **passwords** on your credit card, bank, and phone accounts.
- Keep personal information in your **home** in a secure place.
- At your **workplace, business, doctor's office, or other institutions**, ask what measures they have in place to keep your personal information secure.
- **Don't give out** your personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with.
- Mind your **mail**: deposit your outgoing mail in a post office collection box, rather than in an unsecured mailbox, and have mail promptly removed from your mailbox.
- **Shred** your charge receipts, credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards, and credit offers you get in the mail.
- Don't carry your **SSN card**; leave it in a secure place.
- Guard your **SSN**: only give it when absolutely necessary, and ask organizations to use a different account identifier.
- **Carry only** the identification information and the credit/debit cards that you'll actually need when you go out.
- Be cautious when responding to **promotions**: phony offers may be a ploy to get your personal information.
- Keep your purse, or wallet, and papers with your personal information, in a safe place at **work**.
- When ordering new **checks**, pick them up from the bank instead of having them mailed to your home.
- Keep your **computer**, and the personal information it stores, safe:
  - Use virus protection software and keep it updated.
  - Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know, and be careful about using file-sharing programs.
  - Use a firewall program (especially if your internet connection is constant).
  - Use a secure browser to guard your online transactions. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure.
  - Avoid storing financial information on your laptop unless absolutely necessary. If you do, use a strong password (a combination of letters and numbers and symbols).
  - Before you dispose of a computer, delete all the personal information it stored by using a "wipe" utility program.
  - Check website privacy policies. If you don't see one, or if you don't understand it, consider doing business elsewhere.

(FTC, *Take Charge: Fighting Back Against Identity Theft*; FTC, *Identity Theft: What's It All About*)

Here are some **additional tips** for lowering your risk:

- Have only your first initial and last name printed on your checks. If someone takes your check book, they will not know how you sign your checks (your bank, however, will know).
- When you are writing a check to pay a credit card bill, write only the last four numbers of the account. The credit card company knows the rest of the number, so it will be hidden from others.
- If a phone number is required, consider writing your work phone number on your checks instead of your home number.
- If you have a PO Box, use that instead of your home address on your checks.
- Never have your SSN or Drivers License Number printed on your checks.
- Photocopy the contents of your wallet (both sides of each license, card, etc.) and keep the copy in a safe place. You may also want to keep a photocopy of your passport for when you travel.

Free Annual Credit Reports - The federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months. To order your free annual report from one or all three national consumer reporting companies, go to the **only authorized source**: www.annualcreditreport.com, or call toll-free **877-322-8228**. You should receive it within 15 days.

Other Ways To Obtain Credit Reports - Under federal law, you're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment. You must request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud. Otherwise, a consumer reporting company may legally charge you up to $9.50 for another copy of your report within a 12-month period.

To request or buy a copy of your reports, contact:

- **Equifax**: 800-685-1111 www.equifax.com
- **Experian**: 888-397-3742 www.experian.com
- **TransUnion**: 800-916-8800 www.transunion.com.

If You Become A Victim

If you suspect that your personal information has been used to commit a crime, the Federal Trade Commission advises that you take the following **four steps immediately**:

1. Place a fraud alert on your credit reports, and review your credit reports.

Call the toll-free fraud number of anyone of the three major credit bureaus to place a fraud alert on your credit report. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

- **Equifax** — To report fraud, call: 1-800-525-6285, and write: P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian** — To report fraud, call: 1-888-397-3742, and write: P.O. Box 9532, Allen, TX 75013
- **TransUnion** — To report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

3. File a report with your local police or the police in the community where the identity theft took place.

4. File a complaint with the Federal Trade Commission.

You can file a complaint online at www.consumer.gov/idtheft, or call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653- 4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

The FTC has **additional directions** on resolving fraud related to the following specific issues: Bank Accounts and Fraudulent Withdrawals, Bankruptcy Fraud, Correcting Fraudulent Information in Credit Reports, Credit Cards, Criminal Violations, Debt Collectors, Driver's License, Investment Fraud, Mail Theft, Passport Fraud, Phone Fraud, Social Security Number Misuse, Student Loans, Tax Fraud.

To Find Out More

- FTC website for identity theft: www.consumer.gov/idtheft.
- Federal Department of Justice website for identity theft: www.usdoj.gov/criminal/fraud.
- Mastercard website for identity theft: www.mastercard.com/securityandbasics/identitytheft.
- *Surviving Identity Theft* (Alliance): www.knowdebt.org.