

Identity Theft

Simple Guide to Protecting Yourself

Evelyn Whitmer

Identity thieves are an unfortunate reality in our society. The Federal Trade Commission reports that identity theft tops the list at 37% of complaints. Thirteen percent of the adult population are victims of fraud. It is important to become aware of this problem and take steps to reduce your risk of becoming a victim. An identity thief obtains some piece of your sensitive information and uses it, without your knowledge, to commit fraud or theft against you. Identity theft is a serious crime. Victims have lost job opportunities; been refused loans for education, housing or cars; or even been arrested for crimes they didn't commit. You cannot completely control whether you will become a victim. However, according to the Federal Trade Commission (FTC), you can minimize your risk by managing your personal information cautiously and with heightened sensitivity.

How Identity Theft Occurs

Skilled thieves gain access to your personal information by:

- Getting information from businesses or other institutions by:
 - stealing records from their employer,
 - bribing an employee who has access to these records, or
 - hacking into the organization's computers.
- Rummaging through your trash, or the trash of businesses or dumps.
- Obtaining credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer, or someone else who may have a legal right to the information.
- Stealing credit and debit card numbers as your card is processed by using a special information storage device in a practice known as "skimming."
- Stealing wallets and purses containing identification and credit and bank cards.
- Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.

- Completing a "change of address form" to divert your mail to another location.
- Stealing personal information from your home.
- Posing as a legitimate business person or government official.

Once the thieves have your information, they may go on a spending spree or open new credit card accounts. When they don't pay the bills the delinquent account is reported on your credit report. They may take out loans, obtain wireless service, counterfeit checks or debit cards, open bank accounts, file for bankruptcy under your name and give your name to police during an arrest. (If they don't show up in court, an arrest warrant could be issued in your name.)

Ways to tell if you are a victim of identity theft

Monitor balances of your financial accounts. Look for unexplained charges or withdrawals.

Other indications:

- failing to receive bills or other mail signaling an address change by the identity thief
- receiving credit cards for which you did not apply and/or denial of credit for no apparent reason
- receiving calls from debt collectors or companies about merchandise or services you didn't buy

Steps to take

New accounts show up on your credit report. You can obtain one free annual report from one or all of the national consumer reporting companies; visit www.annualcreditreport.com or call toll-free 1-877-322-8228. Some of the inaccuracies on your credit report may be from computer, clerical, or other errors and may not be a result of identity theft. This is a good time to make sure your credit reports are accurate. If your personal information has been lost or stolen, you may want to check all of your reports more frequently for the first year.

To buy a copy of your credit reports

Equifax: www.equifax.com

1-800-525-6285

Experian: www.experian.com

1-888-EXPERIAN (397-3742)

TransUnion: www.transunion.com

1-800-680-7289

Steps to take to reduce your risk of identity theft

- Place passwords on your credit cards, bank and phone accounts.
- Avoid using easily available information such as your mother's maiden name, birth date and the last four digits of your social security number or your phone number. (Try using a password instead.)
- Secure personal information in your home.
- Ask about security procedures in your workplace. Who has access to your personal information? Are records in a secure location? Ask about disposal procedures for those records.
- Do not give out personal information over the phone, through mail, or over the internet unless you have initiated the contact or you are sure you know who you are dealing with.
- Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or post office. Promptly remove mail from your mailbox. Shred or tear your charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements, and expired charge cards.
- Before revealing any identifying information, ask how it will be used and secured, and whether it will be shared with others. Ask if you can choose to have the information kept confidential.
- Keep your Social Security card in a secure place. Ask if you can substitute your social security number for another number (employee ID number, driver's licence)
- Limit the identification information and the number of credit and debit cards that you carry to what you actually need.
- Keep your purse or wallet in a safe place at work.

Safeguard your computer

- Update virus protection software regularly.
- Don't download files from strangers or click on hyperlinks from people you don't know.
- Use a firewall.
- Use a secure browser-software that encrypts or scrambles information you send over the Internet.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a "strong" password — that is a combination of letters (upper and lower case), numbers, and symbols.
- Avoid using an automatic log-in feature that saves your user name and password and always log off when you're finished.
- Delete any personal information stored on your computer before you dispose of it.
- Read web site privacy policies which should contain information about access security and control of your personal information.
- Report spam e-mail to <http://www.ftc.gov/spam>

What to do if your identity has been stolen

Take the following four steps right away:

1. Place a fraud alert on your credit reports and review your credit reports every three months during the first year.
 - Equifax: 1-800-525-6285; www.equifax.com
P.O. Box 740241, Atlanta GA 30374-0241.
 - Experian: 1-888-397-3742; www.experian.com
P.O. Box 9532, Allen, TX 75013.
 - TransUnion: 1-800-680-7289; www.transunion.com
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.
2. Close any accounts that 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 FTC: www.ftc.gov/idtheft or call toll free 1-877-IDTHEFT (438-4338) or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Reference and Websites of Interest

Farrell, Claudia Bourne, Office of Public Affairs, "FTC Releases Top 10 Consumer Fraud Complaint Categories" <http://www.ftc.gov/opa/2006/01/topten.htm>

Federal Trade Commission, "Consumer Fraud and Identity Theft Complaint Data." Washington, D.C., January-December 2005.

<http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>

Federal Trade Commission, ID Theft, "TAKE CHARGE: Fighting Back Against Identity Theft," booklet. Washington, D.C., June 2005. <http://www.consumer.gov/idtheft>

Shanoff, Carolyn, Associate Director Federal Trade Commission, "ID Theft, What's it all about?" booklet. Washington, D.C., 2004. <http://www.ftc.gov/bcp/online/pubs/credit/idtheftmini.pdf>



THE UNIVERSITY OF ARIZONA
COLLEGE OF AGRICULTURE AND LIFE SCIENCES
TUCSON, ARIZONA 85721

EVELYN B. WHITMER, M.ED.
Extension Agent, Family and Consumer Sciences

CONTACT:
EVELYN WHITMER
emarkee@ag.arizona.edu

This information has been reviewed by university faculty.
cals.arizona.edu/pubs/consumer/az1431.pdf
Originally published: 2007

Other titles from Arizona Cooperative Extension can be found at:
cals.arizona.edu/pubs

Issued in furtherance of Cooperative Extension work, acts of May 8 and June 30, 1914, in cooperation with the U.S. Department of Agriculture, Jeffrey C. Silvertooth, Associate Dean & Director, Economic Development & Extension, College of Agriculture and Life Sciences, The University of Arizona.
The University of Arizona is an equal opportunity, affirmative action institution. The University does not discriminate on the basis of race, color, religion, sex, national origin, age, disability, veteran status, or sexual orientation in its programs and activities.