NOTES

Table of Contents

(continued on next page)

NOTES

Resources

ABC Channel 15, Phoenix, AZ, The Investigators brochure, "Identity Theft Safety Guide". www.abc15.com

Federal Trade Commission www.ftc.gov 1-877-FTC-HELP

Federal Trade Commission Publications:
"Building a Better Credit Record", July 2002.
"ID Theft: What Is It All About," June 2005
"Take Charge: Fighting Back Against Identity Theft", June 2005
"When Bad Things Happen to Your Good Name," November 2003.

Identity Theft: What is it?

Identity Theft is the fraudulent use of another person's identity for some type of gain. This usually takes the form of using another person's identity to obtain credit cards, steal money from bank accounts, apply for loans, obtain a job, rent an apartment, obtain utility or telephone services, or avoid paying fines.

Identity Theft in Arizona is a Class 4 Felony (Taking the ID of another — AZ Rev. Statutes 13-2008).

What information can be used in an Identity Theft?

Any personal information:
- ► Name
- ► Driver's license number
- ► Residential or mailing address
- ► Telephone number
- ► Social security number
- ► Birth date
- ► Military, student or employee number

Are you a potential victim of Identity Theft?

Complete this short quiz to determine your chances of becoming a victim of identity theft.

1. Do you still use your Social Security Number for your photo ID, driver's license number or medical insurance card?
   Yes_____ No_____

2. Is your name listed in the telephone directory?
   Yes_____ No_____

3. Do you leave your vehicle registration and proof of insurance in your vehicle?
   Yes_____ No_____

4. Do you leave your garage door opener in your vehicle?
   Yes_____ No_____

5. Do you carry a purse when you go shopping?
   Yes _____ No_____

6. Do you ever leave your purse (wallet) in a shopping cart, vehicle or in a gym locker?
   Yes_____ No_____

7. Do you place outgoing mail in your home mailbox?
   Yes_____ No_____

8. Do you use "gel" ink in the pens you use to write checks?
   Yes_____ No_____

9. Do you shred all credit card or financial offers you receive in the mail?
   Yes_____ No_____

10. Do you sign the back of your credit cards?
    Yes_____ No_____

Appendix

II. Sample Dispute Letter — For Existing Accounts

Date
Name (*Name of Account Holder)*
Address
City, State, Zip Code

Name (*Creditor, Credit Card Company, etc.)*
Billing Inquiries
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (*charge or debit*) on my account in the amount of $_____. I am a victim of identity theft, and I did not make this (*charge or debit).* I am requesting that the (*charge be removed or the debit reinstated)*, that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of (*use this sentence to describe any enclosed information, such as a police report)* supporting my position. Please investigate this matter and correct the fraudulent (*charge or debit)* as soon as possible.

Sincerely,

Name
Enclosures: (*List what is being enclosed.)*

"Take Charge: "Fighting Back Against Identity Theft", June 2005.

Appendix

I. Sample letter to dispute information found on a Credit Report.

Date
Name (*Name Listed on the Credit Report)*
Address
City, State, Zip Code

Complaint Department
Name (*Credit Bureau)*
Address
City, State, Zip Code

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the report I received. *(Identify items to be blocked by name of sources, such as creditors or tax court, and identify type of item, such a credit account, judgment, etc.)*

Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information from me to block this information from my credit report.

Sincerely,

Name
Enclosures: (*List what you are enclosing.)*

"Take Charge: "Fighting Back Against Identity Theft", June 2005.

11. Do you use a wireless internet connection?
    Yes_____ No_____

12. Do you use on-line banking?
    Yes_____ No_____

13. Do you use your credit card for on-line purchases?
    Yes_____ No_____

14. Do you receive e-mails asking for personal information?
    Yes_____ No_____

15. Have you ever given your credit card number to someone over the telephone?
    Yes_____ No_____

16. Do you use your credit card at stores or restaurants?
    Yes_____ No_____

17. Have you ever filled out an entry form for a contest or a trade show or expo?
    Yes_____ No_____

18. Do you check with your health insurance company once a year to check for unauthorized use or fraudulent billing?
    Yes_____ No_____

19. Have you ever checked with the Social Security Administration to check for unauthorized use of your SSN if you do not now receive W2 wage statements?
    Yes_____ No_____

20. Do you request a credit check from any or all three major credit bureaus at least once a year?
    Yes_____ No_____

Answers on page 22

How Identity Theft Occurs

Arizonians have the dubious honor of having identity theft happen to them more often than anyone else in the United States. One of the reasons is that Arizona has a high population of drug users. Another reason is because identity theft is one of the easiest crimes to commit. It takes no special education, no special talents and no special investment to become an identity thief. It is also one of the most difficult crimes to prevent. There is no way to completely keep our personal information safe. Every single day we interact with others, giving out information that could be used to make us a victim of identity theft or fraud.

Here are some of the ways personal information finds its way into the hands of someone looking to take over some unsuspecting victim's identity:

►Theft of wallets or purses containing credit cards, identification cards and bank account numbers. Wallets left in vehicles, purses left in vehicles or shopping carts are opportunities too good to pass up. Fifty percent of the time an Identity Theft starts with a simple theft of a wallet or purse.

►Theft of mail, from either home mailboxes or trash, including bank statements and bank checks, credit card statements or pre-screened credit card offers, and medical or financial information. Dumpster divers like to hang out in neighborhoods where the residents indiscriminately toss unwanted mail (especially those pesky credit card offers) into their trash. Other mail thieves may follow behind the mail truck as they deliver mail to the boxes that are located at the street and where the majority of the residents aren't able to greet the mailperson.

► A "change of address" form is completed diverting mail to another location. For a One Dollar ($l.00) fee this process can be handled over the internet at the U.S. Post Office site at www.usps.com. However, most ID Thieves request the change of address when completing the new credit application.

► Theft of personal information such as birth certificates,

11. To be secure from outside infiltration, a wireless network must have adequate firewall and encryption protection.
12. On-line banking can be as secure, if not more so, than using checks if the computer and the websites used have adequate encryption (128 bit). Using the bank to pay the bills rather than going to individual sites to make payments protects your account number.
13. Purchases made on-line with a credit card gives you a paper trail of to whom and when the payment was made. Making sure the site has a "lock" and using a low credit limit lessens the risk of a large loss.
14. Most emails asking for personal information are bogus.
15. Before giving your credit card number to a person who has called you requesting a donation, take the time to check to make sure the charity is legitimate through the state's attorney general or online at www.guidestar.org.
16. Every time you use your credit card you are at risk for credit card fraud. By law, stores and restaurants now "truncate" your copy of the receipt showing only the last 4 digits of your card number.
17. Completing an entry form at an expo or contest gives your personal information to one more source, who will probably turn around and sell it.
18. Stealing the use of medical insurance has become big business. Checking payments made for the year can prevent someone from using your coverage.
19. The theft of Social Security Numbers can happen to anyone of any age. It can ruin your credit, prevent you from being able to obtain a loan or keep you from obtaining SSN benefits, and get you into trouble with the IRS.
20. A check of your credit through all three main credit bureaus at a minimum of once a year will help you catch any unauthorized use earlier and keep your credit from being compromised.

Answers to "Are You A Potential Victim of Identity Theft"

1. Your Social Security Number is one of your most valuable pieces of personal information. Using it on anything other than financial or Social Security benefits can compromise your number. Use your SSN only in cases where it is required by law, or if the service provided which needs the number is essential.
2. If you do not want to pay to have your name removed from the phone directory, use your initials, along with your last name, and ask the telephone company to remove your address. Most telephone companies do not charge for this service.
3. Leaving your registration and proof of insurance cards in your vehicle allows anyone breaking into or stealing your vehicle to know 2 pieces of personal information: your name and address.
4. Leaving your garage door opener in your vehicle (along with a copy of your registration) gives the thief a "front door key" to your home since your address is on the registration.
5. Using a fanny pack for shopping allows you to shop without worrying about leaving your purse unattended in a shopping cart, gym locker or car.
6. A purse left in the shopping cart is an opportunity for a thief to reach into it for your wallet, credit cards, cash, etc.
7. Arizona is at the top in statistics for mail theft . The Post Office has closed off many outgoing mail slots in cluster boxes and suggests using only the blue boxes at the post office or shopping centers.
8. Gel ink saturates the paper of the check and is not easily "washed" out.
9. Shredding all credit card offers and financial offers before disposing of them prevents the ID thief from using your credit history to open a new account in your name, but at an address of their choice.
10. Unsigned credit cards are basically invalid. Signing the card also puts your signature on the card rather than the thief's version of your signature, making it easier to spot a forgery.

vehicle registrations, social security records, etc., as the result of a residential burglary or vehicle burglary.

► Theft of information from files that have been improperly disposed of by businesses, educational facilities, health care providers, etc., where the victim may have been a customer, patient, student or employee,

► "Skimming" is the theft of credit card numbers when the card is processed through a portable card reader, usually by employees of service providers, ie: restaurant, retail stores, etc. This skimmer can be hidden under the inside of a belt to be downloaded at a later date into their computer.

► Employee theft of information from files of customer or patient files.

► Information stolen by the use of telephone cameras or other hidden devices which record the PIN numbers or credit card information during transactions in store checkout lines or during ATM transactions.

► Friends, relatives or other trusted individuals that have access to another's personal information, credit cards, PIN numbers, etc.

The internet has assisted the ID Thieves by providing fertile ground to steal personal information from many more victims at one time. Passwords, bank account numbers and other confidential information are being stolen in addition to personal information.

► "Phishing" is the sending of emails that look official requesting personal information.

► "Spoofing" is the sending of a virus or worm contained in an email sent by an infected computer pretending to be a reliable and trustworthy sender.

►"Pharming", the newest and most sophisticated internet scam, "deceives" your local DNS (Domain Name System) server into thinking it has sent your information to the correct website when in reality the information was redirected to another website.

► "War Driving" is the ability to locate wireless systems and using a laptop with special software to "capture" passwords and keystrokes from wireless computers not protected by an adequate encryption program or security.

In the spring of 2005, Phoenix's ABC Channel 15, "The Investigators", produced an in-depth report on identity theft. Included in this report was a survey that was conducted involving inmates in the Arizona Department of Corrections who have been convicted of Identity Theft.* The results of the survey were produced into a brochure entitled, " Identity Theft Safety Guide" and were as follows:

● 66% of the inmates surveyed said they chose their victims at random; A purse left in the vehicle, mail left in an unlocked mailbox and carelessly discarded cash register tapes.

● 33% used the internet to get personal information.

● 31% stole information from mailboxes.

● 38% got their information from garbage— residential trash cans, business dumpsters.

● On the average inmates said that they could steal up to 36 identities in one day and had more than 60 identities at one time. One inmate admitted to having up to 500 identities.

● **Street value of personal information:**
Credit card checks — $150
Canceled checks — $50
Utility bill — $425
Credit Card receipts — $100
Document containing SSN — $1500
Document with date of birth — $1500
Completed Cell phone app — $50

● **91% of the inmates interviewed said they were not afraid of getting caught. ***

*** www.abc15.com**

in the name of the victim, call: SCAN: 1-800-262-7771.

To request that they notify retailers who use their data bases not to accept the victim's checks, call:

TeleCheck: 1-800-710-9898 or 1-800-927-0188
Certegy, Inc.: 1-800-437-5120

Fraudulent New Bank Accounts — If the Identity Thief has been opening accounts contact the banks where the accounts were opened. Also contact: Chex Systems, Inc.: 1-800-428-9623; www. Chexhelp.com

Credit cards — The Fair Credit Billing Act has established procedures for resolving billing errors, including fraudulent charges, on credit card accounts. The law limits liability to $50 of unauthorized charges with conditions:

Write to creditor at the address given for "billing inquiries", NOT the address for sending payments. Include name, address, account number, and a description of the billing error, including amount and date.

The letter must reach the creditor within 60 days after the first bill containing the error was mailed to the card holder. ***If an identity thief changed the address on the account and the card holder did not receive the bill, the dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the billing statement. This is one reason why a card holder must keep track of billing statements and quickly follow-up if bills do not arrive on time.***

The letter should be sent by certified mail, return receipt requested, as proof of the date the creditor received the letter. Include all copies of the police report or other documents. Keep a copy of the dispute letter.

The creditor must acknowledge the complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving the letter.

For information on resolving other issues request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft," from the Federal Trade Commission, www.consumer.gov/idtheft.

"Take Charge: Fighting Back Against Identity Theft.," June 2005

Resolving Specific Problems

Bank Account and Fraudulent Withdrawals — Different laws apply to bank fraud. State laws protect the victim from fraud committed by a thief using paper documents (stolen or counterfeit checks) and federal laws protect the victim when the thief used an electronic transfer of funds (ATM).

If an ATM or debit card is lost or stolen, it must be reported immediately because the amount a victim can be held responsible for depends on how quickly the loss is reported.

- Losses are limited to $50 if the loss or theft is reported within two business days of discovery.
- Losses can be up to $500 if the loss or theft is reported after two business days, but within 60 days after the unauthorized electronic fund transfer appears on a statement.
- If the report is made after 60 days all of the money that was taken from the account after the 60 days may be lost.

Note: Most card issuers voluntarily have agreed to limit or waive consumers' liability for unauthorized use of their debit cards, no matter how much time has elapsed since the disovery of the loss or theft of the card. Contact card issuer for further information.

After receiving the notification of error or fraudulent withdrawal on a statement, the institution generally has 10 days to investigate. Notification of the results of the investigation must occur within 3 days after completion and must correct the error within one day after determining it had occurred. It may take up to 45 days to complete the investigation only if they return the disputed money to the account. It no error is found the money will be withdrawn.

Fraudulent checks and other "paper" transactions — Most states hold the bank responsible for losses from forged signatures or other such transactions, unless the victim fails to notify the bank in a timely manner that a check was lost or stolen.

A victim can contact major check verification companies directly for the following services:

To find out if an identity thief has been passing bad checks

How Identity Thieves Use Your Personal Information

Identity thieves have become very creative in the uses of your identity.

1. They may call your credit card issuer to change the billing address on your account, running up charges that you are unaware of because you are no longer receiving your statements.

2. They may open a new account in your name, "max out" the card and never pay the bill, leaving the company to report your account as delinquent to the credit bureaus.

3. They may establish telephone or cell phone service in your name.

4. They may open a bank account in your name and write bad checks on it, or they may drain your existing bank account.

5. They may file for bankruptcy to avoid paying debts they have incurred in your name or to avoid eviction.

6. They may take out a loan to purchase a vehicle in your name.

7. They may use a fake driver's license using your name with their picture on it for identification.

8. They may give your name to the police when arrested, then never show up for the court date.

9. They may use your identity to collect insurance or medical benefits.

10. They may use your identity to collect on your social security, disability or medicare benefits.

How to Prevent Becoming A Victim

The truth is that even taking all the precautions that can be taken a person may still become a victim of Identity Theft simply because that person shops, pays taxes, buys groceries, etc. In other words, anyone's personal information is available to so many people that there is no way to control all of the places it is used. Many credit bureaus sell it, the phone book lists it, it can even be "googled" on the internet. The best a person can do is make it as difficult as possible for anyone to gain access to it and "keep their fingers crossed."

Here are some things that can be done to protect against identity theft:

√ Avoid giving out your Social Security number. Do not write it on checks or other documents unless it is required for services.

√ Never give personal information, credit card numbers, PIN's or social security numbers to someone over the telephone unless you placed the call.

√ Shred all credit card offers, bank and credit card statements and other personal documents before throwing them away.

√ Use the Postal blue mailboxes to mail outgoing letters and pick up your mail promptly. Avoid using home mailboxes located at the street.

√ Review and reconcile bank and credit card statements on a monthly basis.

√ Do not do on-line banking or other password sensitive activities over a "wireless" network.

√ Check credit bureau activity reports at least once a year, through all three major credit bureaus. Challenge any activity or information on it that is incorrect or unusual.

Steps for Resolving Disputed Information

► Contact both the credit bureau and the creditor, in writing, explaining each item in the report that is believed to be inaccurate. Include copies (not originals) of any documents that support the claim, state the facts, why the items are being disputed and request for a deletion or correction. A copy of the credit report with the information in question circled would help. Send the letter by certified mail, return receipt requested. Document what was sent and when it was received by the credit bureaus. Keep all copies of any letters and enclosures.

► The credit bureau will investigate the items in question, usually, within 30 days. They must also forward all relevant data that was provided about the dispute to the information provider, who must also investigate the claim and report back to the credit bureau. If the information provider finds the disputed information inaccurate, it must notify all nationwide CRAs so they may correct all files.

► Disputed information that cannot be verified must be deleted from a file.

√ If the report contains inaccurate information, the CRA must correct it.

√ If the item is incomplete, the CRA must complete it.

√ If the files shows an account that belongs strictly to another person, the CRA must delete it.

► When the reinvestigation is complete the credit bureau will respond in writing with the results along with a free copy of the credit report if the reinvestigation results in any changes.

► If requested, the credit bureau must send notices to anyone who received a copy of the report within the last six months showing the changes.

► If a creditor or information provider continues to report the disputed information, it must include a notice that the item has been disputed.

"Building a Better Credit Record", FTC, July 2002

All About Credit Reports

The credit bureau is the most common type of Consumer Reporting Agency (CRA). CRAs compile accumulated data into a credit report that is used to determine the "credit worthiness" of potential customers. The information contained in a credit report will remain for varying lengths of time. A bankruptcy, an unpaid line of credit or closed accounts will remain on the credit report for 10 years, while credit inquiries, adverse information, ,judgments, foreclosures and collection accounts will only stay on the credit report for 7 years.

When asked, the credit bureau must give the requestor all information contained in his/her file, including medical information and the sources of the information. In addition, the credit bureau must provide a list of anyone requesting the credit report within the past year and within the last two years for employment related requests.

Another function of the credit bureau is to translate the information contained in the individual credit reports into a three digit number, between 300 and 900, called a credit score. This credit score is the "thumbnail" sketch of a person's level of risk as a borrower and, in many cases, the determining factor if someone is given credit or not. It is the credit score that makes it possible for a person to get "instant" credit at many retail stores. It is also the credit score that is often the indicator that a person has become a victim of identity theft.

In the event of a dispute over information contained in a credit report, a person can protect all of their legal rights by contacting both the credit bureau and the information provider. Under the law, the credit bureau and the organization providing the information to them, such as a bank, credit card company, etc., have responsibilities for correcting inaccurate or incomplete information in an individual's credit report.

Inaccurate information should be challenged and resolved as soon as the discrepancy is found. This can be a very time consuming process since not only the credit bureau records are at issue, but the credit or information provider's records, as well.

You are eligible for a **FREE** Credit Report

A change in the federal Fair Credit Reporting Act (FCRA) now requires each of the nationwide consumer reporting agencies to provide citizens with a free copy of their credit report, at their request, once every twelve months. These agencies are Experian, Equifax and Trans Union.

How to order your FREE credit report

Visit the website:
www.annualcreditreport.com
(***This is the only FREE website, regardless of any other advertising.)***

Telephone: 1-877-322-8228

Mail: Standardized form must be used
(download at : www.ftc.gov/credit)

Mail to: Annual Credit Report Request Services
P.O. Box 105281
Atlanta, GA 30348-5281

What is a credit report????

A credit report contains information on your residency, list of your creditors and your payment history, if you have ever been sued or if you have ever filed for bankruptcy.

This information is sold by the consumer reporting agencies to creditors, insurers, employers and other businesses for their use in evaluating any applications you complete to apply for credit, insurance, employment or home rental.

Protect Your Personal Information

The best way an individual can protect his or her personal information would be to never give it out to anyone for any reason; however, that is being unrealistic. The best a person can do is to try and restrict the amount of information that is available from other sources.

Every year each financial institution or credit card company sends out a "Privacy Notice" which gives the customer the opportunity to limit the use of his or her personal information. Once completed, the customer shouldn't need to make the request again, unless other businesses transactions follow which may negate the original option. The customer should make it a policy to choose the option that provides the most restrictions on the sharing of the personal information.

To "opt out" of receiving pre-screened credit cards and insurance offers from the credit bureau mailing lists call:

1-888-5-OPTOUT (1-888-567-8688)

Or visit:

www.optoutprescreen.com

To remove your name from direct mail lists, send your name, address, and telephone number to:

DMA Mail Preference Service
P.O. Box 643
Carmel, NY 10512

To remove your name from calling lists, send your name, address and telephone number to:

DMA Telephone Preference Service
P.O. Box 1559
Carmel, NY 10512

To place your name on the "**DO NOT CALL**" list

Call: 1-888-382-1222
On-line: www.donotcall.gov

To remove your e-mail address from many direct e-mail lists, visit:

www.dmaconsumers.org

Organizing Your Case

Accurate and complete records will help resolve your identity theft case more quickly. Having a plan of action in place before you start contacting anyone will make sure you get all of the information or help you need.

Prepare a Chart of Action to record of who you talked to and when. The chart will help you keep a log of all contacts in one place in case of questions later.

Make copies of all statements, checks and all correspondence, either received or sent, connected with your identity theft. A "paper trail" is essential when tracking unauthorized access to your identity and your actions to rectify the situation.

Provide copies of all documentation received to date when you make your initial police reports. The more information you can provide at the beginning, the better the chance of finding the identity thief.

Follow up in writing with all contacts you have made on the phone or in person. Use certified mail, return receipt requested for documenting what was sent and when.

Keep the original copies of supporting documents, such as police reports and letters to and from creditors; send copies only.

Set up a filing system for easy access to your paperwork.

Keep old files even if you believe the case has been closed. Problems can still crop up later.

Challenge all inaccurate information on your credit report. Be sure to keep copies of the corrected reports. Have letters available to be included with new credit applications for all information that was not resolved favorably.

CHART OF ACTION

Credit Bureau	Phone Number	Date Contacted	Contact Person	Comments	Comments
Equifax	1-800-525-6285				
Experian	1-888-397-3742				
TransUnion	1-800-680-7289				

Creditor	Address/Phone	Date Contacted	Contact Person	Comments	Comments

Police Agency	Phone Number	Date Contacted	Report Number	Comments	Comments

To remove your name from sweepstakes lists:

Readers Digest: Write requesting no emails, postal mailings from RD and/ or others companies to whom they share their mailing list. Mail to:

Readers Digest
P.O. Box 50005
Prescott, AZ 86301-5005

Publishers Clearinghouse: Write requesting to not receive mailings from both on-line and off-line marketing information sharing. Mail to:

Christopher L. Irving, Sr. Director
Consumer & Privacy Affairs
Publishers Clearinghouse
382 Channel Drive
Port Washington, NY 11050

Credit Bureaus:

Equifax: To obtain a credit report:**
Call 1-800-685-1111
Or write:
P.O. Box 740241
Atlanta, GA 30374-024

Experian : To obtain a credit report:**
Call 1-888-397-3742
Or write:
P.O. Box 2002
Allen, TX 75013

TransUnion: To obtain a credit report**
Call 1-800-916-8800
Or write:
P.O. Box 1000
Chester, PA 19022

** Fee is charged for the report unless it is ordered as the result of filing a report as an Identity Theft victim and provides a “police report number”. There is always a fee charged to obtain the credit score.

What do I do if I become a victim of Identity Theft?*

No matter how many precautions you take, an identity thief could still gain access to your personal information. Make copies of all correspondence, credit card statements, any paperwork that could be used as evidence to the fact that your identity was stolen.

If you suspect you may be a victim of identity theft or fraud take the following steps:

1. **File a report with your local law enforcement agency**. Get the report number, and if, possible, a copy of the police report. You will need this number when contacting creditors or credit bureaus to validate your claim of being a victim. When making the report include information such as: How the Identity Theft was discovered (credit card statement, credit bureau report, SSN benefits canceled, etc.); if the information was compromised as the result of on-line transactions, which site(s) was the information placed (ie: job application, loan application, etc.); did it involve employment history only, was it confirmed by Social Security Administration. Make available any copies of documentation received or showing the fraudulent transactions.

2. **Place a fraud alert on your credit with all three of the major credit bureaus.** Call the toll-free fraud number of any one 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 be notified to place fraud alerts on your account. There will be no charge for this service. Placing a fraud alert on your account will prevent an identity thief from opening additional accounts in your name.

   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-Experian (397-3742), and write: P.O. Box 9532, Allen, TX 75013

   Trans Union — to report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

   Review your credit reports carefully. Look for inquiries not initiated by you, accounts that you did not open, and any unexplained outstanding balances on your current accounts. Also, check that your personal information such as your SSN, address(es), name or initial, and employers are correct. Many inaccuracies are simply due to typographical errors. However, whether due to error or fraud, you should notify the credit bureau as soon as possible by telephone and in writing. Annual checks of your accounts should be made to make sure no new fraudulent activity has occurred. Once the initial fraud alerts expire, you can renew them by contacting each bureau separately.

3. **Close any accounts that have been tampered with or opened fraudulently**. Credit accounts include all accounts with banks, credit card companies and other lenders, telephone companies, utilities, ISP's and other service providers. If you have found new unauthorized accounts call and ask them for their fraud dispute forms. If you find unauthorized charges or debits on an existing account call and ask them for their fraud dispute forms. For the theft or loss of all ATM cards and credit cards and for any replacement accounts always use new Personal Identification Numbers (PINs) and passwords.

   If checks have been stolen or misused, contact your bank immediately. While there is no federal law limiting your losses due to forgery or fraud, many states have laws that may limit your liability if you contact them within a timely manner. Contact your bank for further instructions.

4. **File a complaint with the FTC.** Call: 1-877-IDTHEFT (438-4338), or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or visit: www.consumer.gov/idtheft.

*FTC:ID Theft, What's it all about