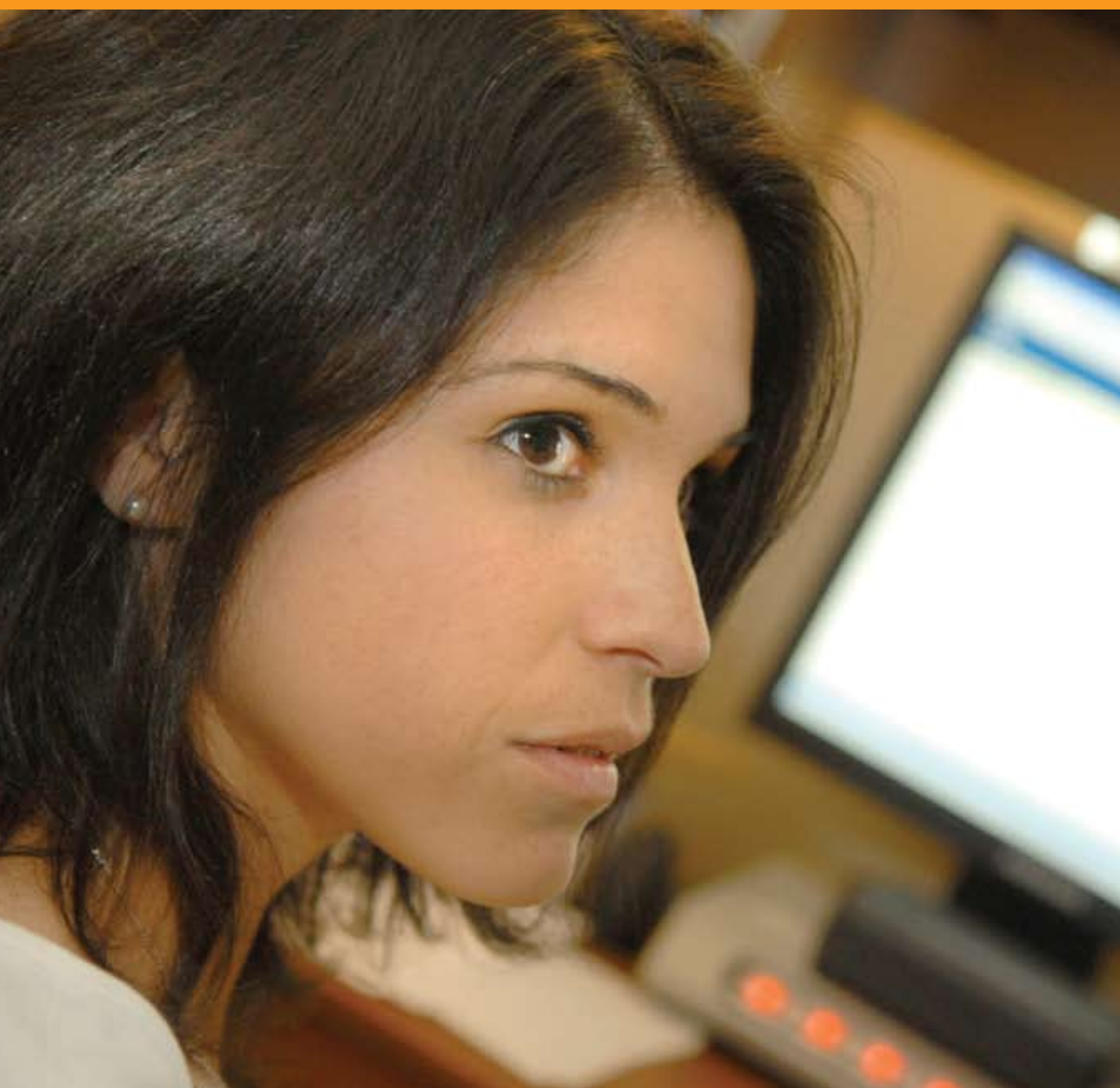
THE USAA EDUCATIONAL FOUNDATION®
Good Information for Good Decisions.®

SAFETY

IDENTITY THEFT



WWW.USAAEDFOUNDATION.ORG®

OUR MISSION

The mission of The USAA Educational Foundation is to help consumers make informed decisions by providing information on financial management, safety concerns and significant life events.

TABLE OF CONTENTS

August 2009

2 WHAT YOU SHOULD KNOW

According to the Federal Trade Commission (FTC), identity theft is the fastest growing crime in America.

For criminals, identity theft is a relatively low-risk, high-reward endeavor. Thieves are difficult to apprehend — and even when caught, are seldom prosecuted.

For victims, it can take months or years and thousands of dollars to clear their good name and credit record. In the meantime, they may be refused loans, lose job opportunities and even be arrested for crimes they did not commit.

That is why it is important to understand what identity theft is, how it happens and how to protect yourself. If you become a victim, your best defense is to recognize it quickly and take immediate action to mitigate its effects. To do so, you must know how to detect identity theft and how to respond if your information is stolen. Do not hesitate to seek appropriate professional advice if legal issues should arise regarding your specific situation.

What Is Identity Theft?

Identity theft occurs when an individual uses your name, address, Social Security number (SSN), bank or credit card statements or other personal information, to commit fraud or other crimes.

Identity thieves work in many ways. They may:

- Open fraudulent bank or credit card accounts in your name, then write bad checks or incur charges.
- Change your billing address, incur charges on your existing credit card accounts and order new credit cards. Because you never receive the bills, you are unlikely to recognize the problem for some time.
- Use your good credit to secure loans.
- Establish wireless phone service in your name.
- Purchase vehicles by securing vehicle loans in your name.
- Use your name and background information to obtain employment.
- Use your name during an arrest for crimes ranging from traffic violations to felonies. If they are released from custody and fail to appear for their court date, an arrest warrant may be issued in your name.

Identity thieves are hard to recognize because they do not necessarily fit a specific profile. An offender could be a complete stranger, a criminally minded cashier or service provider, a neighbor or even a family member.

How Does It Occur?

Identity thieves may use simple means such as stealing your purse or wallet or sophisticated means such as social engineering which is a practice of obtaining information under false pretenses. For example, the identity thieves claim to be calling from a marketing research firm requesting personal information. The information is used to contact your bank or financial institution. The following methods define other forms of identity theft.

Electronic methods include:

- Malware which is malicious software that is harmful to the normal function of computers. It may send personal information on your computer to unauthorized parties via the Internet. You should only download software and updates from sites you know and trust.
- Smishing uses cell phone text messages to deliver a message requiring you to divulge your personal information. Some messages warn that the consumer will be charged unless he cancels his supposed order by going to a Web site that then extracts such credit card numbers and other private data. The method used to actually capture your information in the text message may be a Web site URL; however it has become more common to see a phone number that connects to an automated voice response system.
- Phishing occurs when identity thieves send e-mail or pop-up messages pretending to be financial institutions or other legitimate businesses. The e-mails appear to be authentic, but may contain misspellings and/or grammatical errors. They usually request victims to reveal personal information to avoid an account closure or suspension.
- Vishing is a practice used to convince individuals over the phone to give up personal information by claiming they are your financial institution calling to verify a change or recent transfer you supposedly performed.
- Skimming steals credit or debit card numbers by using a special storage device when processing your card.

Physical methods include:

- Going through trash bins for unshredded credit card and loan applications, discarded credit cards and papers containing personal information such as SSNs, dates of birth or phone numbers.
- Stealing newly issued credit cards, utility bills, insurance statements, benefits documents or other information from unsecured mailboxes.
- Completing a change of address form to divert your mail to another location.
- Posing as a loan officer, employer or landlord to obtain your credit report.
- Stealing files from your employer, merchants, physician's office or other businesses that maintain your personal records.
- Shoulder surfing at automated teller machines (ATM) to capture personal identification numbers (PIN).

Nothing you can do will guarantee protection against identity theft in all circumstances. However, you can minimize your risk by managing personal information with care and caution.

Reduce Access To Personal Data

- Store your wallet or purse in a secure location while at work or in public places such as fitness centers.
- Store personal records such as birth certificates and Social Security cards in a safe deposit box at your financial institution or in another secure location away from your residence.
- Memorize your personal identification numbers (PINs). Never write them on the cards. Do not carry them in your purse or wallet. Never keep the PINs with their cards. Do not share them with anyone, not even with a bank representative, police officer or someone in a store. You are the only one who should know your PINs. If you have a joint account, talk with the joint owner about the importance of keeping it secure. If possible, do not use the same PIN for multiple cards or services.
- Do not share personal information via e-mail or the Internet unless you know and trust the Web site.
- Limit your access to social networking sites as they are often targets for computer security attacks.
- Do not respond to e-mails asking for personal, identifiable information such as SSN, date of birth or mother's maiden name.
- Do not open e-mail attachments or links from unknown individuals.
- Install firewalls on your computer to protect your information.*
- Install software that checks for spyware. (Spyware refers to software that performs certain tasks on your computer, usually without your permission.)*
- Install reputable anti-spam and anti-virus software.*
- Update your firewall, anti-virus and operating systems regularly. In many cases, your system will advise you when it is time to update.

**preferably with automatic update feature*

FOR PRACTICAL TIPS ON PROTECTING YOUR PERSONAL INFORMATION FROM INTERNET FRAUD, VISIT WWW.ONGUARDONLINE.GOV.

- Secure your data when you are using a mobile telephone or wireless laptop by encrypting your wireless connection. This will prevent anyone from connecting to your network and when you are on your local network prevent them from looking at data you are sending out on the net. If your wireless connection is not encrypted, anyone within range can start using your internet connection without your permission.
- Use a cross-cut shredder to dispose of documents with personal or financial information — such as unsolicited loan offers, credit card applications, credit cards, credit receipts or utility bills.
- Cut up or shred data compact discs (CDs) that you are discarding.
- Shield account numbers and PINs from others' view when using credit or debit cards or completing forms at your financial institution.
- Request your local post office hold your mail when you are traveling.
- Use a secured postal mailbox.
- Request online delivery of documents such as bank, credit card, investment or insurance statements.
- Do not display your full name in the phone book and consider an unlisted phone number.
- Do not have unnecessary personal information, such as Social Security or driver's license numbers printed on personal checks.

Protect Your Social Security Number (SSN)

SSNs are a prime target of criminals. If asked to provide yours, always be sure that you are familiar with the business or individual requesting this information.

- Memorize your SSN. Never carry your Social Security card in your wallet or purse.
- Protect pieces of identification that display your SSN.
- Contact your state's Department of Motor Vehicles for replacement drivers' licenses, motor vehicle registrations or identification cards if they display your SSN.

Handle Credit Cards With Care

- Handle credit cards as carefully as you handle cash.
- Thoroughly review monthly credit card statements.
- Never sign an incomplete receipt.
- Copy your credit cards, their account numbers and customer service phone numbers. Keep this information in a secure place, separate from the cards themselves and update it regularly. If your purse or wallet is stolen, you can use this information to notify your financial institutions and credit card companies quickly.

- Keep account numbers confidential. Do not give account numbers to phone solicitors unless properly validated. Do not write them on envelopes, even if space is provided for them.
- When discarding receipts, shred or destroy carbons, which may contain all the information on your credit cards.
- Request PINs or passwords on all your accounts. Follow these tips to create a password.
  - Create passwords with a combination of at least eight letters and numbers, and use both upper- and lower-case letters. Longer passwords are harder to decipher.
  - Think of a phrase or sentence meaningful to you and easy to remember. Then, take the first character from each word, alternate upper and lower case and use some common letter-number substitutions.
  - Avoid the use of personal information as part of your password. Do not use your name, your pet or child's name, your Social Security number or your current or former address.
  - Stay away from number or letter patterns and sequences (for example, "121212" or "abcdefg").
  - Change your password every 60 to 90 days.
  - Vary your password — do not use the same one for every account or retail site.
  - Use a password that differs from your screen name.
  - Do not store your password online.
  - Ask if a passphrase is accepted in place of a password.
- Track the billing cycles of your credit cards so you can follow up if bills are late.

THE USAA EDUCATIONAL FOUNDATION PUBLICATION, *MANAGING YOUR PERSONAL RECORDS*, OFFERS MORE INFORMATION. SEE "RESOURCES" ON THE INSIDE BACK COVER OF THIS PUBLICATION TO ORDER A FREE COPY.

Practice Smart Online Shopping

- Shop only at trusted Web sites. If you are not familiar with a company, do not buy before visiting the Better Business Bureau at www.bbbonline.org to check the company's status. They offer a seal of approval to member companies that promise to abide by certain security and ethical guidelines.
- Make sure the Web site uses encryption technology and begins with https://www. Most Web sites provide some acknowledgement that they are using encryption to transfer financial information. This acknowledgement may appear as a yellow padlock symbol in the status bar of your browser or a pop-up window indicating an encrypted or secured site.

- Be cautious if using your ATM/debit card online, as it provides direct access to your checking or savings account.
- Some credit card companies provide extra protection by issuing a private code or password when shopping online at participating retailers.
- Protect against phishing scams and online fraud when shopping online by only using Web sites that use Extended Validation (EV) certificates. EV certificates give Web site visitors an easy and reliable way to establish trust online. They trigger high security Web browsers to display a green address bar that shows site visitors that the transaction is encrypted and the organization has been authenticated.

RESPONSIBLE COMPANIES TAKE STEPS TO PROTECT THEIR CUSTOMERS FROM IDENTITY THEFT.

Do Business With Responsible Companies

Responsible companies take steps to protect their customers from identity theft. Conduct business with companies that:

- Protect your data. Talk to financial institutions, physicians' offices, schools and other organizations that maintain your personal records. Ask how they handle and store your personal information, if they share this information and for what purpose. Check the privacy policy of the business to determine the nature of its practices.
- Educate customers about protection methods and provide assistance to fraud victims.
- Thoroughly verify customers, especially during high-risk transactions such as address changes.
- Proactively monitor consumer activity and behavior. These companies can alert their customers to sudden, unusual activity in their accounts.

Get Off Promotional Lists

Reduce the opportunity for receiving promotional mail and phone solicitations.

- Call the Credit Reporting Industry Prescreening Opt-Out number at (888) 567-8688 to remove your name from all mailing lists that the agencies supply to direct marketers.
- Contact the Direct Marketing Association at www.dmachoice.org to stop most promotional mail and phone solicitations.
- Register through the National Do Not Call Registry at www.donotcall.gov to stop telemarketing calls.

If you are a victim of identity theft, you can minimize damage to your name, finances and credit history by detecting it early. To do so, you should begin taking the following actions immediately.

Monitor Financial Statements

Carefully monitor activity on your bank, credit card and other financial institution accounts. Review transactions often and carefully for unexplained charges or withdrawals. Dispute anything that looks suspicious. This is the most common way victims discover misuse of their identity. Some banks, credit card companies and financial institutions offer a transaction monitoring service and alerts that electronically notify you when certain account activities occur.

Review Your Credit Report

Order your credit report at least once each year and review it carefully. The Annual Credit Report Request Service is a central contact for requesting your annual credit report. It was created by the three nationwide consumer credit reporting agencies, Equifax, Experian and TransUnion. Visit the site at www.annualcreditreport.com to request a free annual credit report. You are entitled to a free credit report at any time if you have been denied credit, are a victim of identity theft, receive welfare benefits or are unemployed but expect to apply for employment in the next 60 days.

- Make sure all personal information is correct such as names, addresses and phone numbers.
- Make sure all listed accounts are yours.
- Check inquiries on your report to see if they look suspicious or seem excessive.

Examine Your Mail

Scrutinize your mail for signs of identity theft.

- Have you received credit cards for which you did not apply?
- Are financial account statements missing?
- Have you failed to receive new credit cards as expected when current cards are about to expire?
- Have you received letters from debt collectors or businesses about merchandise or services you did not purchase?

If any of these situations arise, follow up quickly with creditors. An identity thief may be tampering with your accounts.

10 IF IT HAPPENS TO YOU

If you determine you have become a victim of identity theft despite your efforts to prevent it, act quickly and thoroughly to minimize the damage. File a report by contacting the police or sheriff's department located where the identity theft took place. Provide as much documented evidence as possible. Make sure the report lists all fraudulent accounts and activities. Keep copies of the report and the investigator's phone number for creditors who require such verification.

Immediate Steps

- Inform your bank, creditors and financial institutions that you are a victim.
  - Ask them to put "fraud alerts" on accounts that have not been compromised. Advise them not to change your address without your written notification and verification. If you do have a change of address or phone number, be sure to notify them, otherwise it may be difficult to obtain credit in the future.
  - Establish new passwords on all accounts.
  - Close existing accounts that have been used fraudulently. Ask if the company accepts the Federal Trade Commission's Identity Theft Affidavit, available at www.ftc.gov/idtheft. If not, ask them to send you a copy of their fraud dispute form, complete it and return it for processing. When opening replacement accounts, use new PINs and passwords.
  - Cancel your ATM/debit card if it has been stolen or compromised. You may be liable for unauthorized charges if fraud is not reported quickly (refer to your ATM/debit card contract). Obtain a new card, account number and PIN.
- Inform the credit reporting agencies that you are a victim of identity theft. To avoid delay, it is strongly recommended that you notify each agency by phone and letter. Ask them to place a "fraud alert" on your credit report to prevent identity thieves from opening accounts in your name. You can place a 90-day initial fraud alert on your credit report which can be renewed in 90-day intervals indefinitely. You can also place an extended fraud alert on your credit report for seven years if you provide a police report or other official record showing that you have been the victim of identity theft. For extra protection you can freeze your credit report. By freezing your credit report you prevent lenders from seeing your credit report unless you specifically grant them access. Be sure and notify them if your phone number changes, otherwise it may be difficult to obtain credit in the future.
- Contact the Federal Trade Commission to report the theft and file a complaint. Your information will be included in a database of identity theft cases that, among other things, aids law enforcement agencies' investigations.
- Notify your employer if you suspect that your payroll and retirement records have been compromised.
- Notify the post office if you suspect that your mail has been stolen, that an identity thief has filed a change of your address with the post office or that a thief has used the mail to commit fraud.

- Contact the Social Security Administration if your Social Security card is lost or your Social Security number has been misused or stolen.
- Notify check verification companies if your checks have been stolen. Ask them to notify their retail partners. Cancel your existing account and request a new account.
- Contact your state's Department of Motor Vehicles office if your driver's license has been stolen or to see if another license has been issued in your name.

Resolving Your Case

As you work with financial institutions and creditors to resolve your case, you may find you are treated with suspicion. Take these steps to protect yourself.

- Take time to understand your rights as a consumer and as a victim of identity theft.
- Keep a log of all conversations — including dates, names and phone numbers — as you deal with legal authorities, financial institutions and credit reporting agencies. You may use the charts provided in the "Reporting Fraud" section.
- Follow up in writing with all contacts you have made over the phone or in person.
- Use certified mail or delivery services where a signature is required for all correspondence regarding your case. Request a return receipt.
- Record the amount of time and out-of-pocket expenses you spend resolving the problem.
- Keep all files, including old ones, even after your case is closed. If identity theft-related errors appear on your credit reports at a future date, you may need your records to dispute them.

LEARN ABOUT FEDERAL AND STATE LAWS, THE ROLES OF LAW ENFORCEMENT AND THE FEDERAL TRADE COMMISSION'S ROLE IN INVESTIGATING AND RESOLVING IDENTITY THEFT AT WWW.FTC.GOV/IDTHEFT.

AS THIS PUBLICATION IS INTENDED FOR GENERAL INFORMATIONAL PURPOSES ONLY, IT SHOULD NOT BE CONSTRUED AS SPECIFIC LEGAL ADVICE. BECAUSE EVERY SITUATION IS UNIQUE, YOU MAY CHOOSE TO SEEK ASSISTANCE FROM AN ATTORNEY OR OTHER QUALIFIED PROFESSIONAL REGARDING YOUR SPECIFIC SITUATION.

RESOLVING IDENTITY THEFT PROBLEMS CAN BE TIME CONSUMING AND FRUSTRATING. IT CAN TAKE MONTHS, EVEN YEARS, TO CLEAR YOUR GOOD NAME AND CREDIT RECORD.

Resolving identity theft problems can be time consuming and frustrating. It can take months, even years, to clear your good name and credit record. In the meantime, you may find it difficult to obtain credit, pay by check, acquire loans or find employment. However, the following laws and procedures have been established to protect you.

Identity Theft And Assumption Deterrence Act Of 1998

This Act makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Federal agencies such as the U.S. Secret Service, the Federal Bureau of Investigation and the U.S. Postal Inspection Service, investigate violations of the Act. These cases are prosecuted by the U.S. Department of Justice.

Gramm-Leach-Bliley Act

According to this Act, the Federal Trade Commission — along with Federal Banking Agencies, the National Credit Union Administration, the Treasury Department and the Securities and Exchange Commission — must issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information.

The Act requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. It also provides an opportunity for customers to limit some sharing of their information.

Your Credit Rights

Under the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act of 2003, you have the right to require a credit reporting agency to do several things to ensure that your credit rating is as accurate as possible.

A credit reporting agency must:

- Provide you with a complete credit report.
- Investigate, at your request, erroneous or missing information in your report. The credit bureau must provide you with a written report of the investigation as well as a revised copy of your credit report if the investigation resulted in changes.
- Keep your credit report information from anyone other than legitimate users of the credit reporting agency.
- Remove detrimental credit information from your file after 7 years. Bankruptcy information can be removed after 7 to 10 years.

When you receive your credit report, you have the responsibility to review it and act on any errors you find.

- Understand the entries on the current report. Each credit reporting agency's credit reports contain information, such as how long an account has been tracked, the highest amount charged, the account balance at the time of the report and the type of account. Other entries identify creditors that have viewed your credit history. Codes indicate debtor's arrangements, repossessions and bad debts, if applicable.
- Ensure your credit report is accurate. Common errors include incorrect personal information, missing information and failing to correct damaging information after the problem is resolved.
- Take action to correct errors. Document your actions and follow up until the problem is resolved.
- Inform creditors of errors. The credit reporting agency must investigate the items in question — usually within 30 days — unless they determine the dispute clearly lacks merit.
- Retain your written account of errors or discrepancies in your file. If an investigation does not resolve your dispute to your satisfaction, you have a right to add a statement to your credit report file contesting the accuracy or completeness of the disputed information.

You may contact your state's Attorney General office or local consumer protection agency for information on your state's identity theft laws. Visit www.naag.org for a list of state offices.

14 MILITARY CONSIDERATIONS

THE USAA EDUCATIONAL FOUNDATION PUBLICATION, *FAMILIES DEALING WITH DEPLOYMENT*, OFFERS MORE INFORMATION. SEE "RESOURCES" ON THE INSIDE BACK COVER OF THIS PUBLICATION TO ORDER A FREE COPY.

As a servicemember, you face unique challenges related to identity theft. Unusual work schedules, frequent relocation and deployment affect your access to normal consumer protection channels.

Active Duty Alert

Active duty servicemembers away from their usual duty station (or a person acting on behalf of or as a personal representative of the servicemember through a power of attorney) may place, at no cost, an active duty alert on their credit report. Active duty alerts remain on your credit report for 1 year unless you request it to be removed. If your deployment exceeds that time frame, you can place another alert in your credit report. While the alert is in effect, creditors must verify your identity before issuing credit in your name, alleviating financial fraud on your accounts. Before you place an active duty alert on your credit report, consider that this may make it more difficult for your spouse to obtain additional credit.

To place an active duty alert, or have it removed, you can call any of the three nationwide consumer credit reporting agencies (Equifax, Experian or TransUnion) listed at the end of this publication.

For more information, visit www.ftc.gov/credit.

Staying Informed

The Military Sentinel is a Web site located at www.ftc.gov/sentinel/military that helps you understand and address forms of identity theft and consumer fraud that may affect you. Military Sentinel's tools include the following.

- Scam alerts to warn you of current fraudulent solicitations for personal information.
- A database that identifies scam artists and others who try to defraud servicemembers.
- Educational materials on understanding credit issues and recognizing fraudulent offers such as work-at-home scams and advance-fee loan scams.
- A secure, online form for reporting identity theft complaints directly to the Federal Trade Commission and Department of Defense officials.

If you become a victim of identity theft, ask your financial institution if they offer an identity theft kit containing form letters and checklists to help you address your situation.

Be sure to include the following information in your communication of the fraudulent event. Since the information that you will be reporting is sensitive, you should protect it by using a confidential envelope for mailing. Keep in mind that some financial institutions may require that you provide a signed and notarized affidavit supporting some of the referenced information below.

Report the fraudulent activity to the following organizations.

1. Credit reporting agencies.
2. Fraud department at each bank or financial institution of each account that has been compromised.
3. Your local police or sheriff's department or police located where the identity theft took place.
4. Federal Trade Commission at www.ftc.gov/idtheft.

Include the following information.

1. Full legal name.
2. Your name used when the fraudulent incident took place.
3. Date of fraudulent incident.
4. Date of birth.
5. Social Security number.
6. Driver's license number or state identification card number.
7. Current address and how long you have lived there.
8. Daytime and evening phone number(s).
9. Describe briefly how the fraud occurred.
10. Indicate your willingness to assist in the prosecution of the person who committed the fraud.

Supporting documentation should include the following.

1. Copy of valid government-issued photo-identification card.
2. Proof of residency when fraud was committed against you.
3. Copy of report you filed with police or sheriff's department.

Sample Letter For Reporting Fraud And Requesting A Block On Your Account

Your Name
Your Mailing Address
Your City, State, Zip Code

Date

Fraud Department
Name of Credit Reporting Agency
Company Address
City, State, Zip Code

Dear Sir or Madam:

I have become a victim of identity theft. I am writing to request that you block the attached fraudulent information on my file. This information does not relate to any transaction that I have made. I have circled the items in question on the attached copy of the report I received.

I am also enclosing a copy of the law enforcement report regarding my identity theft. If you need any other information from me to block this information on my credit report, please contact me.

Sincerely,

Your Name
Home/Work Phone Number(s)
E-mail Address

Enclosures: (List what you are enclosing.)

Sample Letter For Disputing Fraudulent Activity On Your Account

Your Name
Your Mailing Address
Your City, State, Zip Code

Date

Name of Creditor
Billing Inquiries
Address
City, State, Zip Code

Dear Sir or Madam:

I have become a victim of identity theft and am writing to dispute a fraudulent (debit or charge) on my account in the amount of $ _____ . I did not authorize this transaction and am requesting that it be corrected. Please credit any debit, finance and other charges related to the fraudulent amount to my account and send me a corrected statement.

I am also enclosing a copy of the law enforcement report regarding my identity theft and other information to support my position. Please investigate this matter and correct my account as soon as possible.

Sincerely,

Your Name
Home/Work Phone Number(s)
E-mail Address

Enclosures: (List what you are enclosing.)

Recording Your Actions To Report Fraud

The following charts provide a central place where you can record steps you have taken to report fraudulent use of your identity. Keep this information in a secure place for your reference.

RECORDING YOUR ACTIONS TO REPORT FRAUD

CREDIT REPORTING AGENCY	PHONE NUMBER	PERSON CONTACTED	DATE CONTACTED/NOTES
Equifax	(800) 525-6285		
Experian	(888) 397-3742		
TransUnion	(800) 680-7289		

Additional Notes:

FINANCIAL INSTITUTIONS, CREDIT CARD ISSUERS AND OTHER CREDITORS

FINANCIAL INSTITUTIONS	ADDRESS AND PHONE NUMBER	PERSON CONTACTED	DATE CONTACTED/NOTES

LAW ENFORCEMENT AUTHORITIES

AGENCY/ DEPARTMENT	PHONE NUMBER	PERSON CONTACTED	DATE CONTACTED/NOTES
Federal Trade Commission (Identity Theft Hotline)	(877) 438-4338		

20 FOR MORE INFORMATION

The following resources are regularly updated with the most current identity theft information, legislation and means of protection. You should review them periodically to stay informed of issues as they change.

CHECK VERIFICATION COMPANIES

TeleCheck
(800) 710-9898

Certegy, Inc.
(800) 437-5120

FEDERAL TRADE COMMISSION

Identity Theft
(877) 438-4338
600 Pennsylvania Avenue N.W.
Washington, DC 20580-0001
www.ftc.gov/idtheft

SOCIAL SECURITY ADMINISTRATION

Office of the Inspector General
Fraud Hotline: (800) 269-0271
P.O. Box 17768
Baltimore, MD 21235-7768
www.ssa.gov/oig

U.S. POSTAL INSPECTION SERVICE

Mail Fraud
(877) 876-2455
222 S. Riverside Plaza, Suite 1250
Chicago, IL 60606-6100
https://postalinspectors.uspis.gov/

CREDIT REPORTING AGENCIES

Equifax Fraud Division
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian Fraud Division
(888) 397-3742
475 Anton Boulevard
Costa Mesa, CA 92626
www.experian.com

TransUnion Fraud Division
(800) 680-7289
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

Annual Credit Report Request Services
(877) 322-8228
P.O. Box 105283
Atlanta, GA 30348-5283
www.annualcreditreport.com

FOR MORE INFORMATION ON WAYS TO PROTECT YOURSELF AND YOUR COMPUTER FROM IDENTITY THIEVES AND WHAT ACTIONS TO TAKE IF YOU HAVE BECOME AN IDENTITY THEFT VICTIM, VISIT THE FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC) WEB SITE AT WWW.FDIC.GOV/CONSUMERS/CONSUMER/GUARD/INDEX.HTML AND CLICK ON THE MULTIMEDIA PRESENTATION, "DON'T BE AN ON-LINE VICTIM: HOW TO GUARD AGAINST INTERNET THIEVES AND ELECTRONIC SCAMS."

RESOURCES

The USAA Educational Foundation offers the following publications.

INTERNET SAFETY FOR ADULTS (#572)

INTERNET SAFETY FOR TEENS (#573)

MANAGING CREDIT AND DEBT (#501)

BUILDING AND MAINTAINING GOOD CREDIT (#536)

FINANCIAL PLANNING AND GOAL SETTING (#511)

MAKING MONEY WORK FOR YOU (#523)

MANAGING YOUR PERSONAL RECORDS (#506)

BASIC INVESTING (#503)

FAMILIES DEALING WITH DEPLOYMENT (#538)

To order a free copy of any of these and other publications, visit www.usaaedfoundation.org or call (800) 531-6196.

THE USAA EDUCATIONAL FOUNDATION®

WWW.USAAEDFOUNDATION.ORG®

USAA®

USAA is the sponsor of The USAA Educational Foundation.

70520-0809