LIFEGUIDE SERIES

IDENTITY THEFT

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

Table Of Contents

August, 2006

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 account number or other personal information, without permission, to commit fraud or other crimes.

Do not hesitate to seek appropriate professional advice if legal issues should arise regarding your specific situation.

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. The overdrawn or delinquent accounts appear on your credit report.
- Change your billing address and incur charges on your existing credit card accounts. 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.
- Buy 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 or sophisticated means to steal information, such as:

- Taking your wallet.
- Going through trash bins for unshredded credit card and loan applications, 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.
- "Shoulder surfing" at automated teller machines (ATMs) to capture Personal Identification Numbers (PINs).
- Posing as a loan officer, employer or landlord to obtain your credit report.
- Placing malware (malicious software) on your computer that can steal your user IDs, passwords, etc.
- Conducting phone or e-mail scams stating you must provide personal information to claim a prize or update an account.
- Stealing files from your employer, merchants, physician's office or other businesses that maintain your personal records.

These methods are constantly changing and becoming increasingly sophisticated.

Preventing Identity Theft

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 secure location.
- Memorize your 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 necessity for them to have access to your PIN and the importance of keeping it secure. If possible, do not use the same PIN for multiple cards or services.
- Do not provide personal information over e-mail or the Internet unless it is a Web site you know and trust.
  - Install a firewall 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. It may include giving you advertising or collecting personal information about you.)*
  - 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.
  - Do not respond to e-mails asking for personal, identifiable information such as SSN, date of birth, or mother's maiden name. Such inquiries for personal information for fraudulent use are known as "phishing."
  - Check the Web site address (URL) to ensure you are on the correct site and have not been redirected to a fraudulent site.
  - Do not open e-mail attachments or links from unknown individuals.
  - For practical tips on protecting your personal information from Internet fraud, visit www.onguardonline.gov.
- Buy a cross-cut shredder. Use it as a secure means of disposal for 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 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.
- Directly deposit checks to your checking or savings account. Do not mail checks from your home mailbox if it is unsecured.

* *preferably with automatic update feature*

- Consider getting a post office box or locked 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. Consider getting an unlisted number.
- Do not provide personal information over the phone unless the recipient is a known and trusted source.
- Do not have unnecessary personal information, such as social security or driver's license numbers, printed on personal checks.

Protect Your Social Security Number

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, such as health insurance cards, just as you would your ATM/debit or credit cards. Take them out of your wallet only when you need them. Otherwise, keep them out of public sight.
- As of January, 2005, states can no longer display SSNs on drivers' licenses, motor vehicle registrations or other state identification cards. If your current state's driver's license, motor vehicle registration or identification cards contain your social security number, consider contacting your state's Department of Motor Vehicles for replacements of necessary items.

Handle Credit Cards With Care

- Treat credit cards as carefully as you treat cash.
- Do not put your address, phone number or driver's license number on credit card sales receipts.
- Thoroughly review monthly financial 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 bill envelopes, even if space is provided for them. Do not make them available to unauthorized individuals.
- When discarding receipts, shred or tear up carbons, which may contain all the information on your credit cards.
- Ask if you can put PINs or passwords on all your accounts. Make up a fictitious word or use an alphanumeric password (typically at least 6–8 characters long) that you will remember.

- Do not put your credit card account number on the Internet unless it is encrypted on a secured site as described in the following "Practice Smart Online Shopping" section.

- Always keep credit card receipts that display your entire account number secure — never throw them into a public trash can. When shopping, put receipts in your wallet rather than in the shopping bag.

- Track the billing cycles of your credit card(s) so you can follow up if bills are late.

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 checking 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 to safeguard your information. 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.

Do Business With Responsible Companies

Responsible companies take steps to protect their customers from identity theft. Conduct business only with those 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, whether they share this information and for what purpose. Check the Privacy Promise of the business to determine the nature of its practices. Does the business live up to its promises and procedures?

- Educate customers about protection methods and provide assistance to fraud victims.

- Take care to thoroughly authenticate 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.

- 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.dmaconsumers.org to stop most promotional mail and phone solicitations.

Detecting Identity Theft

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 every statement from your bank, credit card company and other financial institutions. Review transactions carefully for unexplained charges or withdrawals. Dispute anything that looks suspicious. This is the most common way victims discover misuse of their identity.

Carefully monitor every statement from your bank, credit card company and other financial institutions.

Review Your Credit Report

Order your credit report at least once each year and review it carefully. You can request and receive a free credit report **annually** from any of the three credit reporting agencies. These agencies also sell various financial products and services, which you are not required to purchase.

- 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 bills or 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.

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 police report by contacting your local police, or sheriff's department or police 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.

Phone numbers, addresses or Internet addresses necessary to complete the following steps are listed in the "Resources" section of this publication.

Important

Inform the credit reporting agencies that you are a victim of identity theft.

Immediate Steps

- Inform your bank, financial institutions and creditors that you are a victim.
  - Ask them to put "fraud alerts" on accounts that have not been compromised and not to change your address without your written verification.
  - Establish new passwords on all accounts.
  - Close existing accounts that have been used fraudulently. Ask if the company accepts the FTC's Identity Theft Affidavit, available at www.consumer.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. Contact each one by phone and letter. If you inform one credit reporting agency that you are an identity theft victim, it is obligated by federal law to notify the other two agencies within 45 days. To avoid delay, it is strongly recommended that you notify each agency yourself.
  - Ask them to place a "fraud alert" on your credit profile to prevent identity thieves from opening accounts in your name. You may need to provide information — such as proof of your identity, a copy of a police report or a signed statement from you regarding fraudulent activity — before they will put the alert on your file.

- Request a copy of your credit report and review it carefully. You can request and receive a free credit report **annually** from any of the three credit reporting agencies. These agencies also sell various financial products and services, which you are not required to purchase. You are entitled to a free credit report **at any time** if you are a victim of identity theft, have been denied credit, receive welfare benefits or are unemployed.

- The Annual Credit Report Request Service is a centralized contact for individuals to request annual credit reports. 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.

- Close new, unauthorized accounts that appear on your credit report. When speaking to the credit company, ask if they accept the FTC's Identity Theft Affidavit, available at www.consumer.gov/idtheft.

  If not, ask them to send you a copy of their fraud dispute form, complete it and return it for processing.

- Act quickly if you find transactions that are not yours. Contact each company involved and request copies of their records relating to the fraudulent activity.

- Contact the FTC 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. You may visit www.consumer.gov/idtheft for more information.

- 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 SSN 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

Unfortunately, in many identity theft cases, victims must prove their innocence. 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:

- Learn about federal and state laws, the roles of law enforcement and the FTC's role in investigating and resolving identity theft at www.consumer.gov/idtheft.

- 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.

- Do not pay bills that are not yours. Such action could be viewed as admittance that the bill is yours.

- To ensure you are not held liable for fraudulent activity in your name, you should consider the following:

  - Do not pay any bill or portion of a bill that is a result of fraud.

  - Do not cover any checks written or cashed fraudulently.

  - Do not file for bankruptcy. Your credit rating should not be permanently affected and no legal action should be taken against you.

  - Report any merchant, financial institution or collection agency to the FTC immediately if they attempt to coerce you into paying fraudulent bills or threaten to take legal action against you.

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.

Do not pay bills that are not yours.

Understanding Your Rights

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, write checks, 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.

The Act also requires the FTC to serve as a central clearinghouse for identity theft complaints. The FTC must log and acknowledge complaints, provide victims with relevant information and refer complaints to appropriate law enforcement and reporting agencies.

Gramm-Leach-Bliley Act

According to this Act, the FTC — 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 inform customers of their privacy policies at least annually. Before disclosing any personal financial information to a third party, financial institutions must notify the consumer and provide an opportunity for the individual to opt out of such disclosure.

Your Credit Rights

Under the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions (FACT) 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. You are entitled to a free credit report **at any time** from any of the agencies if you have been denied credit, are a victim of identity theft, receive welfare benefits or are unemployed. You can request and receive a free credit report **annually**.
- 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 7–10 years.

When you receive your credit report from the credit reporting agencies, make sure:

- You understand the entries. Each 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 debtors' arrangements, repossessions and bad debts, if applicable.

- Your credit report is accurate. Most frequent errors include incorrect personal information, missing information and failing to correct damaging information after problems are resolved.

- You take action to correct errors. Document your actions and follow up until the problem is resolved.

- You inform creditors when errors are identified. The credit reporting agency must notify all creditors who have viewed your credit history during the past 6 months of errors in your file.

- You retain your written account of errors or discrepancies in your file if an investigation does not resolve your dispute.

State Legislation

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.

Active Duty Alert

Active duty servicemembers (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 in their credit report. Active duty alerts remain in your credit report for 1 year unless you request it to be removed. If your assignment 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.

To place an active duty alert, or have it removed, you can call any of the three nationwide consumer reporting agencies (Equifax, Experian or TransUnion) listed in the "Resources" section at the end of this publication. You will need to provide proof of your identity which could include your SSN, name, address or other personal information.

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

Military Considerations

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

Staying Informed

The FTC and Department of Defense (DoD) created Military Sentinel, a Web site at www.consumer.gov/military that helps you understand and address forms of identity theft and consumer fraud that may affect you. Military Sentinel's tools include:

- Scam alerts to warn you of current fraudulent solicitations for personal information.
- A database that identifies scam artists and others who try to defraud members of the military community.
- 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 FTC and DoD officials.

Protection While Deployed

If deployment is a possibility, you should select a trusted, experienced individual to help administer your financial affairs in the event you are deployed. Execute the proper power of attorney to enable this individual to prevent, detect and respond as needed to identity theft during your deployment. Whether you choose a spouse, parent, friend or financial professional, make sure you:

- Select an individual you know and can trust to manage your affairs with integrity — someone who will devote time and attention to your finances.
- Select an individual who understands the details of your financial situation and is capable of managing your financial affairs accurately and responsibly.
- Spend time discussing the details of your financial situation with this individual. He should be familiar with details such as the content of your mail, bank statements and credit card statements so he can identify unusual or suspicious activity.
- Check with your installation's legal officer or attorney when discussing these issues so that you execute the most appropriate power of attorney that will meet your financial needs. Your financial institution may also have the appropriate forms available for your completion and review by your legal adviser.

Reporting Fraud

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. Please 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

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:

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 Address
Your City, State, Zip Code
Your Account Number

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 make 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

Enclosed: (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			
Name Of Organization	Address And Phone Number	Person Contacted	Date Contacted/Notes

Law Enforcement Authorities				
Agency/ Department	Phone Number	Person Contacted	Report Number	Date Contacted/Notes
FTC (Identity Theft Hotline)	(877) 438-4338			

Resources

The following Web sites are regularly updated with the most current identity theft information, legislation and means of protection. You should review them periodically to stay abreast of these 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 Ave. N.W.
Washington, DC 20580
www.consumer.gov/idtheft

Social Security Administration

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

U.S. Postal Inspection Service

Mail Fraud
(800) 372-8347
222 S. Riverside Plaza, Ste. 1250
Chicago, IL 60606-6100
www.usps.com/postalinspectors/fraud

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
P.O. Box 9532
Allen, TX 75013
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 (centralized contact for individuals requesting annual credit reports)
(877) 322-8228
P.O. Box 105281
Atlanta, GA 30348
www.annualcreditreport.com

Important

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."

Notes

Notes

Research Hints

There is a wealth of information on this topic that can be further researched at your local or college library, or on the Internet. The Internet is a wonderful research tool where you can find sites that provide general information, related links and resources that can help you in your search. Log onto a search engine and type in keywords of the subject matter that you are researching. If you explore the numerous sites on the Internet, you should be able to strengthen your research and find information that will fit this subject. The USAA Educational Foundation has not reviewed and cannot guarantee the accuracy of any other Internet Web sites.

Tip

When researching on the Web, make sure that your source is a reliable and known entity.

The USAA Educational Foundation offers the following related publications:

Managing Credit And Debt (#501)

Basic Investing (#503)

Personal Records (#506)

Financial Planning And Goal Setting (#511)

Making Money Work For You (#523)

To order a free copy of any of these publications, call (877) 570-7743 or visit www.usaaedfoundation.org.

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.

THE USAA EDUCATIONAL FOUNDATION℠

WWW.USAAEDFOUNDATION.ORG®

USAA®

USAA is the sponsor of The USAA Educational Foundation.

70520-0806