

IDENTITY THEFT – WHAT IT IS AND HOW TO AVOID IT

1. What is Identity Theft? Identity theft may be defined as the illegal, fraudulent use of your name, date of birth, and social security number and other identifying information unique to you, used by another individual in order to obtain goods, services, merchandise, cash, or property. The [Center for Social & Legal Research](#) noted in a study that in 2002 there were about seven (7) million victims of identity theft in the United States alone. This LAPA will review developments in the area of identity theft, explain the typical scenario for identity theft and prevalent scams, explain what steps one can take in order to prevent being the victim of identity theft, and provide the service member with a number of contacts and resources in order to fight back if he has been the victim of identity theft. Finally, this LAPA will also provide some general guidelines in evaluating legitimate and non-legitimate companies and scams commonly aimed at the military that the member should be on the lookout for and thus should avoid.

Comment [M1]:

2. Why target the Military: Why are military members such good targets for predators who proliferate scams upon the unsuspecting consumer? In short, this is true because military members have a steady source of income that is consistently paid twice per month. In particular, the following factors may also play a role: 1) military members are strongly encouraged and counseled to pay all just debts; 2) Many military members are fairly young and lack the financial expertise and savvy to identify a poor financial deal; and 3) If the service member defaults on his debt or loan, it is usually easier for the debt collector to track the service member.

3. What criminals do with your personal information:

- Gain access to your personal accounts, change your mailing address, and provide false information to your creditors.
- Open new bank accounts in your name and establish utility service in your name using your Social Security number and date of birth.
- File bankruptcy under your name in order to avoid paying debts that they created.
- Create checks and debit cards in order to withdraw money from your bank account.
- File fraudulent tax returns.
- Obtain driver's licenses and other identification in your name.
- Use insurance information in order to obtain medical treatment.
- Take out loans in your name in order to purchase expensive homes and automobiles.

4. Can the consumer avoid being the victim of Identity Theft? Yes. Since identity theft is basically a crime of opportunity the consumer should be wise to take the following precautions in order to combat identity theft:

- Avoid carrying your Social Security number, PIN numbers or passwords in your wallet or purse.
- Do not have your Social Security number printed on your checks.
- Make a photocopy of everything in your wallet and keep it in a secure place.
- Avoid giving out personal information over the telephone, through the mail or through the Internet unless you personally know the contact or initiated the contact yourself.
- Find out how your personal information will be used before you disclose it to others. Ask the company if the information can and will be kept confidential.
- Give your Social Security number if and only if it is necessary. Ask to use an alternate source of identification. Always avoid putting your Social Security Number and date of birth on person web pages or publicly posted resumes.
- Avoid using your Social Security number as your driver's license number.
- Use good passwords on your credit card, bank, and telephone accounts. Avoid using pet names, mother's maiden name, your date of birth, and the last four digits of your Social Security number.
- Never use your home mailbox to deposit outgoing mail. Instead, deposit all outgoing mail in the post office collection boxes or at your local post office. If you plan to be away from home and can't find someone to pick up your mail for you, arrange with the Postal Service to hold your mail at your local post office until you can pick it up (1-800-275-8777). This practice should be followed in order to discourage mail theft.
- Promptly review all of your bills and bank statements when they arrive at your home. Check the statements for any errors or inconsistencies.
- Never deposit or throw documents that contain sensitive information in the dumpster or recycling bins. Thieves who steal from trash or recycling bins are known as "dumpster divers". All documents that contain sensitive personal information such as credit card receipts, physician statements or bills, telephone and other utility bills, bank statements, expired credit cards, and credit card pre-approval offers that you receive in the mail, should all be placed in the shredder. In other words, shred and destroy.
- Safeguard where you leave personal information in the home especially if you employ help from outside the home, such as a maid, home repair, or other similar employment. This may also include when you have service contractors come in your home in order to make repairs.
- Determine who has access to your personal information and work and confirm that this information is kept in a safe and secure location.
- Watch your credit. Order copies of your credit report every year from each of the three major credit reports agencies. They are: 1) Equifax, P.O. Box 105851, Atlanta, GA 30348, 800-685-1111, <http://www.equifax.com>; 2) TransUnion, P.O. Box 1000, Chester, PA 19022, 800-888-4213,

<http://www.transunion.com>; and 3) Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, <http://www.experian.com>. Do not delay in reporting any errors in your credit report.

- Subscribe to an online credit monitoring service that will notify you within 24 hours of any changes to your credit file.
- Call 1-888-5OPTOUT in order to stop the pre-approved credit offers from coming to your home. This may not prevent all of the offers from coming to your home, but prevents most of them.
- Lock it up. Your government ID and driver's license should be in a safe and secure place at all times. If necessary, lock your desk, cabinets and safe where such information is located.
- Watch out for those strange ATM machines. ATM machines may be used to skim data off your card's magnetic strip, which may be used later to clean out your bank account.
- Watch out for "shoulder surfers" when using pay telephone or public Internet access. Your free hand should be used to block the view of the keypad. Avoid using cordless phones to conduct sensitive transactions since cordless phone are prone to eavesdroppers on other phones picking up the conversation.
- Install firewalls and anti-virus detection software on your home computer. For more information about computer security see <http://www.staysafeonline.info>.
- Before you make any online purchases or conduct online banking check the privacy and security policies of the Web sites. Never respond to unsolicited e-mail requests for personal information.
- Watch out for Internet accounts that look official but are not. Recent scams have been run through EBAY and YAHOO look-alikes. Most recently a military member discovered that he was using the mypay website to try to download an LES. This is not the official DFAS website and he was entering his SSN in the search bar to retrieve his LES. This website is a fraudulent web site and unsuspecting members and those not paying close attention could enter their SSN and make themselves the victim of ID theft. The real DFAS web site to retrieve personal pay information is <http://www.dfas.mil/>.

5. What should the consumer do if he becomes the victim of Identity Theft? If you are an identity theft victim, the following is a call to action to declare war on the criminal:

- Report the crime immediately. You must file a police report with your local police department or local sheriff's department. Obtain a copy of the report number for future reference.
- File a complaint with the Federal Trade Commission (877-ID-THEFT). Download a copy of the ID theft affidavit from the FTC's web site at <http://www.consumer.gov/idtheft>.
- For fraud involving your mail file a complaint with the U.S. Postal Service at <http://www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm>.

- Contact the three major credit-reporting agencies and place a fraud alert on your account: Equifax, 800-252-6285 or www.equifax.com; Experian, 888-397-3742 or www.experian.com; and TransUnion, 800-680-7289 or www.transunion.com.
- Notify all banks, credit unions, creditors, and utilities that have extended you credit or otherwise have opened an account in your name. Be prepared to provide these companies with a copy of the police report. Cancel or rescind all PIN numbers or passwords.
- Contact the Internet Fraud Complaint Center (IFCC) to report the theft of your identity at: <http://www.ic3.gov/default.aspx>
- Obtain a copy of your credit report on an annual basis from all three credit bureaus.
- Depending on the nature of the fraud, you may consider contacting the following agencies:
- Social Security Administration: 800-269-0721 or <http://www.ssa.gov>.
- Local Post Office and United States Postal Inspector: <http://www.usps.gov>
- Federal Bureau of Investigation (FBI): If the fraud crosses state lines, then contact the FBI at <http://www.fbi.gov/contact/fo/territory.htm>.
- United States Secret Service: If counterfeit checks are involved, contact the Secret Service at <http://www.ustras.gov/uss/>.
- United States Department of State: If your passport is lost or stolen, contact the State Department at <http://www.state.gov>.
- Internal Revenue Service (IRS): <http://www.irs.gov>.

6. Other Helpful **Links** are as follows:

[ACLU Privacy Issues](#)

[The Campaign to Stop Junk Email](#)

[Electronic Privacy Information Center](#)

[Equifax CreditWatch](#)

[Experian Fraud Center](#)

[Federal Bureau of Investigation](#)

[Federal Communications Commission](#)

[Federal Trade Commission Identity Theft](#)

[Identity Theft Resource Center](#)

[Identity Theft Survival Kit](#)

"Identity Theft: What to Do If It Happens to You"

Internal Revenue Service

Military Sentinel

U.S. Department of Justice

U.S. PIRG

U.S. Postal Inspection Service

8. In any and all cases involves identity theft you cannot afford to sit back and fail to act. Act and act you must if these criminals are going to be brought to justice and stopped in their tracks. Remember, in cases involving identity theft, time is of the essence. If you wish to share your views about identity theft with your local or federal representatives, visit the Consumers Union public policy web site at www.consumersunion.org/. Please contact your local Legal Assistance Office with any additional questions about identity theft.