



ASA DIX LEGAL BRIEF

A PREVENTIVE LAW SERVICE OF THE JOINT READINESS CENTER LEGAL SECTION
UNITED STATES ARMY SUPPORT ACTIVITY DIX
KEEPING YOU INFORMED ON YOUR PERSONAL LEGAL NEEDS

IDENTITY THEFT

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name. The rigors of military life can compound the problems that identity theft creates.

Q: What is identity theft? Identity theft occurs when someone obtains a piece of your sensitive information, like your Social Security number, date of birth, address, and phone number, and uses it without your knowledge to commit fraud or theft.

Q: How do identity thieves get my personal information? Skilled identity thieves use a variety of methods to gain access to your personal information. For example, they may steal records while on the job, rummage through your trash, obtain your credit report through fraud, steal credit card numbers, change your mailing address to receive credit card and bank statements, or simply steal your wallet or purse.

Q: How do identity thieves use my personal information? Once identity thieves have your personal information, they may go on spending sprees using your credit/debit accounts, open new credit accounts, take out auto loans in your name, establish phone service in your name, drain your bank account, open a new bank account and write bad checks on that account, or give your name during an arrest.

Q: How can I deter identity theft? You can deter identity thieves by safeguarding your information, especially if you live in barracks or with roommates. Shred financial documents and paperwork with personal information before you discard them. Protect your Social Security number and military identification card. Be cautious when giving out personal information over the telephone, internet or through the mail. Use firewalls, anti-spyware, and anti-virus software to protect your home computer and keep them up to date. Do not use an obvious password like your birth date, your mother's maiden name, or the last four digits of your social security number. Do not let mail pile up unattended if you cannot collect it. Use a mail stop, P.O. Box, or have someone you trust hold your mail while you are away.

Q: How can I detect if I have been a victim of identity theft? You can detect suspicious activity by routinely monitoring your financial accounts, billing statements, and credit report. Be alert to warning signs such as bills that do not arrive as expected, unexpected credit card statements, denials of credit for no apparent reason, calls or letters about purchases you did not make. If you are unable to take these steps while you are deployed, consider placing an "active duty alert" on your credit report to help minimize the risk of identity theft while you are deployed. To place an alert on your credit report or to have it removed, you will have to provide appropriate proof of your identity, including your Social Security number, name, address, and other personal

information requested by the consumer reporting company. You may use a personal representative to place or remove an alert. When a business sees the alert on your credit report, they must verify your identity before issuing any credit. As part of this verification process, the business may try to contact you directly. Be sure to keep your contact information updated or you may experience delays if you are applying for new credit. When you place an active duty alert on your credit report, you will also be removed from the credit reporting companies' marketing list for prescreened credit card offers for two years unless you ask to be put back on the list before then. To place an active duty alert, contact one of the three consumer reporting companies at the following numbers: Equifax: 1-800-525-6285, Experian: 1-888-EXPERIAN (397-3742), TransUnion: 1-800-680-7289.

Q: How can I defend myself once I have been a victim of identity theft? If you have been a victim of identity theft, you should immediately place a fraud alert by contacting one of the three companies listed above. Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you cannot explain. Close any accounts that have been tampered with or established fraudulently, and use new pins and passwords when you open new accounts. Call the security department of each company where an account was opened and ask for verification that the disputed account has been closed and the fraudulent debts discharged. Always follow up any phone conversations in writing by certified mail. File a police report with local law enforcement, which will help you with creditors who may want proof of the crime. If the local police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. Explain the situation to your commanding officer so there are no surprises if creditors contact your superiors looking to collect charges made by the identity thief. Be sure to report the theft to the Federal Trade Commission. You can file a complaint online at www.consumer.gov/idtheft; or call: 1-877-IDTHEFT (438-4338); or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

ASA DIX LEGAL BRIEF is one of a series of Information Papers from the ASA Dix Joint Readiness Legal Section containing general legal information on topics which Legal Assistance Attorneys frequently advise on. Information provided is general in nature and does not constitute formal, specific legal advice. Consult an Attorney for specific legal advice for your particular situation. You may schedule a legal assistance appointment by calling the Joint Base Legal Assistance Division at 609-754-2010. February 2010