IDENTITY THEFT

Adapted from an article by 8th Army Legal Assistance Office

Identity theft is the crime in which one uses your personal data for fraudulent or deceptive purposes, usually to obtain economic gain. Unlike fingerprints, personal data such as your social security number, credit cards numbers, and telephone card numbers can be taken from you and used to your disadvantage. The harm you might suffer can be greater than the immediate economic loss. It can also include ruining your reputation, criminally and financially.

How can I avoid becoming a victim of identity theft?

Below are things you can do to prevent becoming a victim:

a. Adopt a "need to know" approach to personal information. Unless you trust the person, or they have a good reason why they need your personal information, avoid disclosing it.

b. Check your financial statements as soon as they are available. Look at your bank records, telephone records, and credit card records to see if there are any unexplained charges, withdrawals or phone calls. If there is, contact the company that issued the statement as soon as possible.

c. Review a combined copy of your credit report (all three reporting agencies) annually. Check your credit report for any unexplained accounts opened in your name. If such accounts exist, write to the credit-reporting agency as soon as possible.

d. Keep copies of all bank and financial statements for at least one year. These documents may help you resolve identity theft related disputes should you become a victim.

e. If you are sending a check via mail, do not put it in your mailbox. Rather, drop it off at the post office or a USPS mailbox.

f. Cancel all credit cards that you have not used within 6 months.

g. Avoid "Dumpster Divers". Do not throw away important documents, such as credit card receipts or pre-approved credit applications. Shred these documents to ensure that thieves will not be able to use them against you.

h. Look out for "Shoulder Surfers", i.e., people who will look over your shoulder while you are using an ATM to get your PIN number.

i. The next time you order checks, do not put your signature block on them. Using your initial will not allow the thief to determine how you sign your names on your checks.

j. Do not sign the back of your credit card; however, certain merchants may not accept an unsigned credit card (e.g. the United States Postal Service). If a clerk actually checks for a signature, be prepared to show photo identification. NEVER have your social security number printed on your checks.

k. Keep a record of all the information you carry in your purse/wallet. If it is ever lost or stolen, you will know who to call and cancel accounts.

l. When you check out of a hotel that uses cards for keys, do not turn in the key. The cards contain all the information you gave the hotel, including address, credit card numbers and expiration dates. Someone with a card reader, or employee of the hotel, can copy the information on the card.

If I become a victim of identity theft, what can I do?

Get the records you maintained on your creditors and banks accounts. Then call each to provide notice of the theft and have the appropriate action taken, including canceling the accounts.

a. Contact the Federal Trade Commission (FTC). The FTC has been charged with the responsibility of receiving and processing complaints from individuals who may have been victims of identity theft. The FTC will also help refer your complaint to the appropriate entities that can help you. For more information go to www.ftc.gov.

b. File a police report immediately. This shows credit providers that you were diligent and have started taking the necessary action to minimize the loss. This also begins the investigation.

c. Call the three national credit reporting agencies IMMEDIATELY to place a fraud alert on your name and social security number. Once the alert is placed, creditors know that your information was stolen and will contact you before creating an account in your name.

    1) Equifax, P.O. Box 74201, Atlanta, GA 30374-0241. Tel: (800) 685-1111.
    www.equifax.com/

    2) Experian, P.O. Box 4500, Allen, TX 75013, 866-617-1894.
    www.experian.com

    3) Trans Union, PO Box 390, Springfield, PA 19064, 800-888-4213.
    www.tuc.com

d. If an account has already been established in your name fraudulently, contact the creditor and instruct them to close the account. Inform the creditor that you are a victim of identity theft.

Active duty Fraud Alerts

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports. To do so, contact any one of the three major consumer reporting companies (page 2). Active duty alerts can help minimize the risk of identity theft while you are deployed. When a business sees the alert on your credit report, it must verify your identity before issuing any credit.

To place an alert on your credit report, or to have it removed, you will need to provide appropriate proof of your identity, including your SSN, name and address. You may use a personal representative to place or remove an alert. Active duty alerts remain in effect for one year, unless you request that it be removed earlier. If your deployment lasts longer than one year, you may place another alert on your credit report.

If I have other questions, what should I do?

Please contact the Legal Assistance Office on Torii Station at 652-4332.