Defense Privacy and Civil Liberties Office

GUIDELINES ON COMBATING IDENTITY THEFT

The Department of Defense takes very seriously its obligation to protect the personal information of the millions of military and civilian personnel who daily work to support our nation's defense, and I assure you that we are working harder than ever to prevent, identify and mitigate information breaches. Attached you will find a guide for preventing, recognizing, and fighting back against identity theft.

Time is of the essence when dealing with identity theft, and it is important that you know your rights, responsibilities, and necessary actions to protect yourself against unnecessary harm. This guide will walk you through steps you can take to safeguard your personal information as well as those necessary to defeat identity theft when it does occur. I hope you will find this information helpful. Thank you for aiding in the battle against identity theft.

The following information was compiled from the Federal Trade Commission Identity Theft website at www.ftc.gov/idtheft .

What is Identity Theft?

Identity theft is a rapidly growing crime that exploits your personal information in order to open false accounts in your name, or to access your current accounts fraudulently. Identity thieves can accrue thousands of dollars of debt in your name and leave you and your family to foot the bill. Additionally, identity theft can leave your credit record in shambles, making it harder to qualify for loans, and possibly jobs, in the future. Identity thieves can commit crimes in your name, leaving you with a criminal record. Most identity theft begins with seemingly innocent events. A stolen wallet or checkbook can easily turn into a stolen identity, and missing personnel records can give thieves a gold mine in personal information. Identity theft can come from many sources.

- Stealing mail, checks, or personnel records.
- Dumpster Diving: Rummaging through trash for bills or other personal documents.
- Changing Your Address: Using change of address processes, thieves can divert mail, including bank statements, credit card statements, and credit offers in order to access your information and accounts.
- Phishing: A popular method of information theft, phishing entails sending fraudulent emails claiming to be from financial institutions or companies needing your personal information. Phishing can include redirecting you to official looking 'dummy' websites that gather your information, under the pretext of reputable financial institutions – often your own bank or credit company.
- Skimming: At stores or restaurants that you frequent, your personal and credit card information could be in jeopardy. Identity thieves can use technologically advanced card readers to collect your information from credit cards which they process for your everyday purchases. Waiters

or clerks can scan your card when you make purchases and save the information for later manipulation.

How Can I Prevent Identity Theft?

For Active Duty Military Personnel deployed away from their usual duty station and who do not anticipate seeking new credit while deployed, you may want to issue an "Active Duty Alert" on your credit report. Effective for one year, Active Duty Alerts require creditors to take extra steps to verify your identity before granting credit in your name. You can remove Alerts before one year if necessary, as well as extend an alert when it is set to expire. To place an Active Duty Alert, call the toll-free fraud number of one of the three nationwide consumer reporting companies (Equifax, Experian, and TransUnion) – the company you ask to place the alert is required to contact the other two. You may use a personal representative to place or remove an alert.

There are many other recommended steps that you can take to prevent identity theft.

- Shred documents containing personal or financial information.
- Protect your Social Security Number. Don't carry your card in your wallet, and don't give out your number unless certain it is necessary and it will be kept secure.
- Don't give out personal information over the phone, mail, or Internet unless you know the recipient and their intended usage, and are absolutely certain it is secure.
- Safeguard your military ID.
- Never lend credit cards or share account information.
- Don't click on links in unsolicited emails. Type web addresses you know directly into the browser instead. If in doubt about the authenticity of an email from a financial institution contact the institution directly.
- Secure your computer. Keep security software active and up to date. Use complex, secure passwords, not obvious words, dates or numbers such as a mother's maiden name, birth date, or social security number.

What are the Signs of Identity Theft?

The most important prevention method for identity theft is always personal vigilance. Catching and stopping identity theft in its early stages – or before it has even begun – is the best way to protect your money and your reputation. You should monitor your financial accounts closely for irregularities or fraudulent expenses, and check your credit reports annually for errors. Additionally, watch out for these telltale signs of identity theft.

- You notice that bills do not arrive as expected or at all.
- You receive unexpected credit cards or account statements for accounts you did not open.
- You receive calls or letters about purchases you did not make.
- You are denied credit for no apparent reason.

What do I do if I Suspect Identity Theft?

If you suspect that you have become a victim of identity theft you should move quickly to prevent further intrusions into your personal information and your financial accounts. Begin by calling the toll-free fraud number to one of the three nationwide consumer reporting companies (numbers available on back page) and asking them to place a "Fraud Alert" on your credit reports.

A Fraud Alert will put in place a 90 day period of advanced protection measures on your accounts. Creditors will be required to follow extra procedures before opening new accounts in your name or making changes to your existing accounts, hopefully preventing further breach of your accounts.

Additionally, filing a Fraud Alert entitles you to one free credit report from the three credit reporting companies (Equifax, Experian, and TransUnion). Check this free report for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. If you find inaccurate or fraudulent information, contact the consumer reporting companies to get it removed.

What do I do if My Identity is Stolen?

If you discover that your identity has been stolen and fraudulent accounts have been opened in your name, or fraudulent purchases made from your accounts, there are several steps which can help you defend against the crime and its potentially devastating aftereffects.

- Close Any Accounts Opened or Used Fraudulently – Call and speak with the security or fraud department of each company for instructions on closing your accounts and opening new accounts. Follow up in writing, and include copies (NOT originals) of supporting document. Send letters by certified mail, return receipt requested, so you can document what the company received and when.

  If the identity thief made charges or debits on your accounts or on fraudulent accounts, ask the company for the necessary forms to dispute transactions. If the company does not have special fraud dispute forms, write a letter to dispute the fraudulent charges. In order to dispute the charges on new unauthorized accounts, fill out the Federal Trade Commission's ID Theft Affidavit form at www.*ftc.gov/idtheft* and mail it to any company or financial institution holding a fraudulent account. Ask the company for written confirmation that the disputed account has been closed and the debts removed.

- File a Police Report – Contact your local police department to file a report. Be sure to get a copy of the police report, or at the very least, the number of the report. If police are hesitant to take a report, ask to file a "Miscellaneous Incidents" report or contact another jurisdiction, such as county or state police.

- For Military Personnel, Notify Your Commanding Officer of the Problem – Alerting your Commanding Officer to the problem may save some confusion should creditors call looking to collect on fraudulent charges.

- Place an "Extended Alert" on your Credit Report – After confirming that someone has unlawfully accessed your account or used your information to open fraudulent accounts, you can place an extended alert on your credit report. This will require submitting an Identity Theft Report to verify you have been subject to identity theft. Extended alerts last for a period of seven years and will require businesses to verify your identity before issuing you credit – including contacting you directly. This may delay your attempts to obtain credit, but will make it difficult for thieves to open accounts in your name.

- Request a "Credit Freeze" – Many states have laws that allow consumers to freeze their credit, restricting access to your credit report. If you decide to place a freeze on your credit, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Credit freeze laws vary from state to state and can include fees for placing, lifting, and temporarily removing freezes. Credit Freezes must be filed with each of the three credit reporting agencies (Equifax, Experian, and TransUnion).

- File a Report with the FTC – Visit www.ftc.gov/idtheft to file a complaint with the Federal Trade Commission. By filing with the FTC, you will provide valuable information that could help law enforcement officials track down and stop identity thieves.

Additional Measures that May be Necessary

- In some extreme instances, identity theft may require canceling government issued identifications. Lost driver's licenses or other forms of identification can still be used by thieves to access your information or otherwise harm your reputation. If your government issued IDs have been stolen, call the issuing office to cancel the card and reapply for a replacement. Also ask the agency to flag your file so that no one else can get a license or any other personal identification document in your name.

- Social Security Numbers – If after doing everything in your power to clear up the effects of identity theft you discover someone is still fraudulently using your Social Security Number, you can request a new number. Requesting a new Social Security Number comes with its own problems, however. A lack of associated credit history with the new number could affect your ability to obtain credit and loans. Your credit information should transfer with a new number. To apply for a new Social Security Number you must prove that you continue to be the victim of Identity Theft.

Credit Reporting Companies:

Equifax
www.equifax.com
1-800-525-6285

P.O. Box 740241
Atlanta, GA 30374-0241

Experian
www.experian.com
1-888-EXPERIAN (397-3742)

P.O. Box 9532
Allen, TX 75013

TransUnion
www.transunion.com
1-800-680-7289

Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

Federal Trade Commission

www.FTC.gov/IDTheft
1-877-ID-THEFT (438-4338)
TTY: 1-866-653-4261

Identity Theft Clearinghouse
Federal Trade Commission
Washington, DC 20580