United States Army
Criminal Investigation Command

Media contact: CID Public Affairs Office
703-806-0372

For Immediate Release

CID Lookout
On Point for the Army

Learn to Protect Yourself from Identity Theft

CID Special Agents share tips to deter, detect and defend against fraud

FORT BELVOIR, Va., September 26, 2007 – Special Agents of the U.S. Army Criminal Investigation Command, commonly known as CID, are helping Soldiers, family members and Army civilians learn to recognize the warning signs to deter, detect and defend themselves from becoming targets of identity theft and consumer fraud.

With billions of dollars lost and millions of Americans as victims, consumer fraud and identity theft is the number one complaint for consumers in the United States. CID defines identity theft and identity fraud as any type of crime involving the fraudulent use of someone's personal identifying information, such as s social security number, date of birth, or bank account number to commit a crime.

According to a 2007 Federal Trade Commission (FTC) annual report on consumer crime, identity theft is a vicious crime that can continue well beyond someone losing their money or personal property; it's a crime that can rob innocent men and women of their good credit, reputation and financial well being, without them even knowing it has occurred.

Commonly, the identity thief will use this information for financial gain, often taking control of someone's personal finances, obtaining credit cards, making purchases on-line, and taking out loans, all within one's name, but can also obtain and incur services charges such as cell phone bills and rental car fees. Even worse is when the imposter commits crimes using the identity of someone else and gives that person a criminal record.

On average the identity theft victim doesn't realize they are a victim for approximately 12 months and often spends the next couple of years trying to repair the damage the imposter has done to their credit, reputation, and financial well being.

Military members and their families can be targets for identity thief. Much of their personal information is contained in documents needed to conduct daily business. From identification cards, vehicle registrations, TDY and PCS orders to DD Form 214 (Certificate of Release or Discharge from Active Duty), all contain personal information that needs to and should be safeguarded.

Some of the common ways identity theft can occur involves skilled identity thieves using a variety of methods to steal personal information. According to CID Special Agents and the FTC, some of the methods include:

- **<u>The Scam</u> - Dumpster Diving**

  This involves rummaging through trash looking for bills or other personal information. Thieves will collect the information, piece torn documents together and use it to steal your identity. **What to do -** Shredding or burning bills or documents with your personal data will help prevent identity theft. Also destroy any pre-approved credit card applications received in the mail.

- **<u>The Scam</u> - Pretext Calling**

  Pretext calling is the fraudulent means of obtaining a person's personal information needed to impersonate someone. The pretext caller through deception poses as a bank employee, law enforcement official, or other authority figures and through innocent sounding questions and queries collects personal identifying information needed to further their crime. A pretext caller may contact financial center employees, posing as clients, accessing the clients' personal account information changing addresses so as not to alert the person being victimized until it is too late. The callers can then withdraw, divert or create fraudulent accounts without the victim's knowledge. Not only are the banks being contacted but also employers and even the victim themselves. **What to do -** Avoid the pretext caller, be cautious to whom you provide your personal information and for what purpose. Never give out personal information over the phone or Internet unless you initiated the contact or know the person to whom the information is being provided. When at work and someone calls trying to get personal information about an employee, ask for their name and number then verify prior to providing any information. Most of this seems like common sense; however, these pretext callers are experts in the execution of their scam and sound very convincing.

- **<u>The Scam</u> - Card Skimming**

  This method involves the unauthorized copying of electronic data from your credit or debit cards through the use of hidden equipment like cameras, false PIN pads on ATM machines, or card readers. **What to do -** To protect yourself, use your hand or body to prevent people from looking over your shoulder while at an ATM or a debit card Point of Sale terminal. Look for any physical alterations at the ATM or debit card locations.

- **<u>The Scam</u> – Phishing**

  Identity thieves known as "phishers" send email or "pop-up" messages claiming to be a legitimate business or organization like a bank, Internet service provider, online payment service, or government agency. The urgent message directs the victim to a familiar-looking web site to "update" or "validate" their account information, which will then be used to run up bills or commit crimes in their name. **What to do -** To avoid phishing scams, don't use email, instant message, or chat room links to get to any web page if you suspect the message might not be authentic or you don't know the sender or user. Avoid filling out forms in email messages that ask for personal financial information and ensure you're using a secure website when submitting credit card or other sensitive information via your web browser.

- **<u>The Scam</u> – Vishing**

  This is a relatively new scam that uses Voice over Internet Protocol, or "VoIP" phones to steal financial information. "VoIP" is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. "Vishing" is a combination of "voice" and "phishing," which is short for "voice phishing." Con artists send blast e-mail or recorded phone messages that appear to be from a financial institution, payment service or other well-known business. The message reports a "security" problem and urges the victim to call a telephone number to "fix" their account. The victim thinks it's safer calling a telephone number than to click on an unknown imbedded hyperlink. **What to do - Do** not automatically trust a phone number based on its area code. Con artists can hack into Caller ID systems and VoIP users can assign any area code to a phone number. To avoid becoming a victim of this scam, do not give out your PIN numbers or passwords, especially if you receive a recording that refers to you as a "valued customer" instead of your name. These are warning signs since legitimate institutions would never ask you to verbalize

your PIN or passwords. If you have to check your card legitimately, don't call a number they provided you, call the number on the back of your card or recent bank statement.

- **<u>The Scam</u> - "Old-Fashioned" Theft**

  Wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information are likely targets of theft that can lead to identity theft. **What to do -** Consumers can place fraud alerts with their credit card companies and are mainly effective against new credit accounts being opened in your name. But, fraud alerts have their limitations and will likely not stop thieves from using your existing accounts, or opening new accounts such as new telephone or wireless accounts, where credit is often not checked. If you suspect you're a victim of identity theft, report it immediately to your local law enforcement, financial institution or agency where the discrepancy was discovered.

- **<u>The Scam</u> - Changing Your Address**

  Billing statements and other personal information can be diverted to another location by a thief completing a "change of address" form. **What to do -** The Postal Service has safety devices in place to inform the consumer that a change of address has taken place by sending a confirmation notification to both the old and new addresses. Consumers then have the ability to correct the action if they did not initiate the address change.

Additional Tips

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. Do not cut and paste the link in the message.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system.
- Soldiers who do not expect to seek new credit while deployed also have the option placing an "active duty alert" on their credit report while away from their duty stations. The alert requires creditors to take steps to verify your identity before granting credit in your name and is effective for one year, unless requested to remove sooner. If a deployment lasts longer than a year, another alert can be added on your report.
- CID Special Agents recommend consumers become aware of the signs that identity theft has occurred. Some examples include: bills are late or missing, receiving credit cards that were not applied for, being denied credit or offered less favorable terms for no apparent reason, or when getting contacted by debt collectors or others about purchases that were not made.

The FTC recommends your credit report be reviewed and checked for inaccuracies at least once a year by calling the toll-free fraud number of any one of the three nationwide consumer credit bureaus:

- Equifax - www.equifax.com - 800-685-1111.
- Experian - www.experian.com - 888-397-3742.
- Trans Union - www.tuc.com - 800-916-8800.

# # #

Editor's note: To download high resolution versions of the CID Lookout logo visit http://www.cid.army.mil/lookout_logos.html

CID Lookout is a U.S. Army Criminal Investigation Command (USACIDC) initiative to partner with the Army community by providing a conduit for members of the Army family, to help prevent, reduce and report felony-level crime.

The USACIDC, commonly known as CID, is an independent criminal investigative organization that investigates serious, felony-level crime such as murder, rape, sexual assault, robbery, arson, fraud, and even cyber crime or intrusions into the Army networks (see CID Cyber Lookout).

Solving and preventing these types of crime cannot be achieved solely by CID Special Agents and the Military Police. Together, professional law enforcement officers and the Army community must work hand-in-hand to fight serious crime. As such, CID is *On Point for the Army* and depends heavily on Soldiers, family members and civilian employees to *Be On The Lookout* and provide assistance in keeping the *Army Strong* and safe.

CID Lookout provides the latest information to the Army community aimed at helping Soldiers protect themselves, their families and to reduce their chances of becoming crime victims.

For more information on CID or to report a felony-level crime or provide information concerning a crime, contact your local CID Office or the Military Police, or visit www.cid.army.mil.