

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

For Immediate Release



## CID warns, beware of email scams Although warnings heavily publicized, crooks still persist, victims still fall prey

**FORT BELVOIR**, **Virginia**, July 23, 2008 – The U.S. Army Criminal Investigation Command is warning the Army community to beware of foreign scams or advanced fee fraud, using unsolicited faxes, email or letters to obtain money or personal information. CID also wants to make the public aware of the criminal implications for Army personnel who actively facilitate these schemes.

These foreign scams, also known as the "Nigerian Scam," the "Iraq Scam," the "Foreign Lottery Scam" and the "419 Scam" begin with someone from overseas making unsolicited contact with unsuspecting victims requesting their help in disposing of gold or money recovered from Saddam Hussein in Iraq, or oil revenues from Nigeria or Russia, or lottery winnings from some other foreign location. Other contacts request help to negotiate U.S. Postal Money Orders or traveler's checks that later turn out to be forgeries or counterfeit. The perpetrator uses false names - sometimes even using the names of real Soldiers - or steals another person's identity and then fraudulently uses that identity.

In most instances, if the victim responds to the proposals, they are asked to do something to show good faith with the person who sent the message. In the case of money orders and traveler's checks, the person is asked to cash the checks, told to keep a percentage of the funds for themselves, and to send the remaining money to an overseas address.

In the case of gold or money dispositions, the victim is sometimes asked for personal identification, to include bank account numbers, or as the scam progresses, the victim is asked to send money to pay for unexpected fees (hence the name, advance fee fraud) that are needed to bribe an official or free up a process so that the gold or money can be transferred.

Soldiers and civilians who knowingly participate in the negotiation of fraudulent money orders or traveler's checks in furtherance of fraud schemes are subject to Title 18 of the U.S. Code, Section 1343, *Fraud by Wire, Radio or Television*. The title states that individuals who devise schemes to defraud, obtain money or property under false pretenses, representations or promises will be fined or imprisoned for up to 20 years, or both. Violators that affect financial institutions can be imprisoned for up to 30 years, fined up to \$1 million, or both.

According to CID Special Agents, email fraud provides unique challenges for law enforcement personnel, Soldiers, Army civilians and family members. Criminals can mask their identities, locations and cover their tracks quickly. Web sites can easily be established and removed in very little time, allowing scam artists to strike quickly and disappear even faster.

CID officials remind individuals to never provide their personal identification, bank account numbers, or other financial information to an unsolicited request. The unknown source could use the information to the financial harm of the victim. Never travel to foreign locations to meet with the individuals conducting these schemes for any reason. Victims have often been robbed, kidnapped, or even killed, when lured to other countries.

The United States Secret Service (<a href="www.ustreas.gov/usss/">www.ustreas.gov/usss/</a>) and the United States Postal Service (<a href="http://postalinspectors.uspis.gov/">http://postalinspectors.uspis.gov/</a>) are the primary U.S. law enforcement agencies dealing with these types of scams. U.S. citizens or residents who <a href="mailto:have not">have not</a> suffered a financial loss and want to report a scam may forward unsolicited emails to the USSS at <a href="mailto:419.fcd@usss.treas.gov">419.fcd@usss.treas.gov</a>. U.S. citizens and residents who <a href="mailto:have not">have</a> suffered a financial loss should contact the nearest field office of the Secret Service by telephone.

Victims are advised to continue reporting these fraudulent scams to law enforcement agencies.

-30-

**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 provides 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 <a href="https://www.cid.army.mil">www.cid.army.mil</a>.