

United States Army Criminal Investigation Command

Media contact: CID Public Affairs Office 571-305-4041

FOR IMMEDIATE RELEASE

With National Spotlight on Internet Romance-Type Scams, Army CID Makes Additional Attempts to Warn Unsuspecting Victims

QUANTICO, Va. Jan 25, 2013 – In light of recent national news coverage, the U.S. Army Criminal Investigation Command, commonly known as CID, is again pleading with internet users worldwide to not fall prey to the ongoing online "Romance Scams" that the Army has been combating since 2009. Army CID is hopeful that the recent coverage can potentially help warn victims of the cyber-crime that ends in both undue heartache and financial hardship.

CID special agents continue to receive hundreds of reports from victims located around the world regarding various scams of persons *impersonating* U.S. Soldiers online. Victims are usually unsuspecting women, 30 to 55 years old, who believe they are romantically involved with an American Soldier, yet are being exploited and ultimately robbed by perpetrators that strike from thousands of miles away.

"We cannot stress enough that people need to stop sending money to persons they meet on the internet and claim to be in the U.S. military," said Chris Grey, Army CID's spokesman. "It is heartbreaking to hear these stories over and over again of people who have sent thousands of dollars to someone they have never met and sometimes have never even spoken to on the phone."

The majority of the "romance scams," as they have been dubbed, are being perpetrated on social media, dating-type websites where unsuspecting females are the main target.

The criminals are pretending to be U.S. servicemen, routinely serving in a combat zone. The perpetrators will often take the true rank and name of a U.S. Soldier who is honorably serving his country somewhere in the world, marry that up with some

2-2-2 Romance Scams

photographs of a Soldier off the internet, and then build a false identity to begin prowling the internet for victims.

"We have even seen instances where the Soldier was killed in action and the crooks have used that hero's identity to perpetrate their twisted scam," said CID Special Agent Matthew Ivanjack, who has fielded hundreds of calls and emails from victims.

The scams often involve carefully worded romantic requests for money from the victim to purchase special laptop computers, international telephones, military leave papers, and transportation fees to be used by the fictitious "deployed Soldier" so their false relationship can continue. The scams include asking the victim to send money, often thousands of dollars at a time, to a third party address.

Once victims are hooked, the criminals continue their ruse.

"We've even seen instances where the perpetrators are asking the victims for money to purchase "leave papers" from the Army, help pay for medical expenses from combat wounds or help pay for their flight home so they can leave the war zone," said Grey.

These scams are outright theft and are a grave misrepresentation of the U.S. Army and the tremendous amount of support programs and mechanisms that exist for Soldiers today, especially those serving overseas, said Grey.

Along with the romance type scams, CID has been receiving complaints from citizens worldwide that they have been the victims of other types of scams – once again where a cyber crook is impersonating a U.S. servicemember. One version usually involves the sale of a vehicle; where the servicemember claims to be living overseas and has to quickly sell their vehicle because they are being sent to another duty station. After sending bogus information regarding the vehicle, the seller requests the buyer do a wire transfer to a third party to complete the purchase. When in reality, the entire exchange is a ruse for the crook to get the wire transfer and leave the buyer high and dry, with no vehicle.

Army CID is warning people once again to be very suspicious if they begin a

Romance Scams

3-3-3

relationship on the internet with someone claiming to be an American Soldier and within a matter of weeks, the alleged Soldier is asking for money, as well as their hand in marriage.

Many of these cases have a distinct pattern to them, explained Grey.

"These are not Soldiers, they are outright thieves. If someone asked you out on a first date and before they picked you up they asked you for \$3,000 to fix their car to come get you, many people would find that very suspicious and certainly would not give them the money. This is the same thing, except over the internet." said Grey.

The perpetrators often tell the victims that their units do not have telephones or they are not allowed to make calls or they need money to "help keep the Army internet running." They often say they are widowers and raising a young child on their own to pull on the heartstrings of their victims.

"We've even seen where the criminals said that the Army won't allow the Soldier to access their personal bank accounts or credit cards," said Grey.

All lies, according to CID officials.

"These perpetrators, often from other countries, most notably from West African countries are good at what they do and quite familiar with American culture, but the claims about the Army and its regulations are ridiculous," said Grey.

The Army reports that numerous very senior officers and enlisted Soldiers throughout the Army have had their identities stolen to be used in these scams.

To date, there have been no reports to Army CID indicating any U.S. service members have suffered any financial loss as a result of these attacks. Photographs and actual names of U.S. service members have been the only thing utilized. On the contrary, the victims have lost thousands. In one extreme example, a woman from New York took out a second mortgage on her home to get money to help her "Soldier." She lost more than \$60,000. More recently, a woman from Great Britain told CID officials she had sent more than \$75,000 to the con artists.

"The criminals are preying on the emotions and patriotism of their victims," added Grey.

4-4-4 Romance Scams

The U.S. has established numerous task force organizations to deal with this and other growing issues; unfortunately, the people committing these scams are using untraceable email addresses on "Gmail, Yahoo, Hotmail," etc., routing accounts through numerous locations around the world, and utilizing pay-per-hour Internet cyber cafes, which often times maintain no accountability of use. The ability of law enforcement to identify these perpetrators is very limited, so individuals must stay on the alert and be personally responsible to protect themselves.

"Another critical issue is we don't want victims who do not report this crime walking away and thinking that a U.S. serviceman has ripped them off when in fact that serviceman is honorably serving his country and often not even aware that his pictures or identity have been stolen," said Grey.

What to look for:

- DON'T EVER SEND MONEY! Be extremely suspicious if you are asked for money for transportation costs, communication fees or marriage processing and medical fees.
- If you do start an internet-based relationship with someone, check them out, research what they are telling you with someone who would know, such as a current or former service member.
- Be very suspicious if you never get to actually speak with the person on the phone or are told you cannot write or receive letters in the mail. Servicemen and women serving overseas will often have an APO or FPO mailing address. Internet or not, service members always appreciate a letter in the mail.
- Many of the negative claims made about the military and the supposed lack of support and services provided to troops overseas are far from reality – check the facts.
- Be very suspicious if you are asked to send money or ship property to a third party or company. Often times the company exists, but has no idea or is not a part of the scam.
- Be aware of common spelling, grammatical or language errors in the emails.

5-5-5

Romance Scams

Where to go for help:

Report the theft to the Internet Crime Complaint Center (IC3) (FBI-NW3C Partnership).

Online: http://www.ic3.gov/default.aspx

Report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the United States in their investigations.

Online: http://www.ftc.gov/idtheft

By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

Report the fraud to the Federal Trade Commission on Nigerian Scams.

Email: <u>spam@uce.gov</u>

For more information on CID visit www.cid.army.mil

-30-