United States Army
Criminal Investigation Command

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

FOR IMMEDIATE RELEASE

CID Lookout
On Point for the Army

CID warns of extortion and blackmail scams

Quantico, Va., Nov. 3, 2015 – For many, the words extortion and blackmail bring forth images of Hollywood movies, celebrities having illicit affairs and corporations trying to hide a wrongdoing. In today's world of Internet communications, Internet dating, and social networking, extortion and blackmail can happen to anyone who discusses, admits, or posts a lapse in judgment or their personal or financial issues over the Internet. More alarming, extortion and blackmail can happen to innocent individuals whose personal information has been stolen as part of a data breach.

The U.S. Army Criminal Investigation Command, commonly known as CID, warns the Army community to be aware of Internet extortion and blackmail scams and report any instance where a Soldier, Army dependent, or Army civilian is or has been faced with threats involving the payment of money or other valuables.

Extortion and blackmail are crimes that have grave consequences for its victims, to include financial loss. The FBI's Internet Crime Complaint Center 2014 Internet Crime Report stated that more than $16 million dollars was extorted from victims that year.

"In many instances, the situation begins when an unknowing victim is befriended by someone on the Internet, often as part of an online dating or social media site," said Daniel Andrews, director of CID's Computer Crime Investigative Unit. "The scammer quickly builds a friendship and trust with the victim, and will begin to ask for or discuss information or photos that could be hurtful to one's personal or professional life if revealed. Because

-more-

the victim does not realize they are being scammed, they see the requests or discussion as a normal part of the developing friendship and are willing to share the information."

To the victim's surprise, Andrews said, the scammers then threatens to release that information if money is not paid.

Another instance of extortion can occur when scammers obtain an individual's personal information as part of a data breach. Such breaches, according to the Identity Theft Resource Center, occurred 591 times in the first nine months of this year alone, compromising more than 175 million records.

"Following a data breach, these scammers, these criminals, may try to extort money from individuals who have a personal, financial, or medical condition they would not want exposed," Andrews said.

The FBI report gave one example, called payday loans, deferred-deposit check loans or cash advance loans, as the most abundant type of extortion scam reported. The scam takes place when an individual's personal information has been revealed to what may appear to be a legitimate business. The scammer calls the individual notifying them that a loan in his or her name is delinquent and must be paid in full to avoid legal consequences. The scammer has accurate information, such as social security numbers, birth dates, bank account numbers, etc., and poses as a representative of a legitimate agency collecting debt. The scammer often refuses to provide details of the alleged loan and may become abusive when questioned. The FBI report further states that victims are often threatened with legal action, arrests, and in some cases physical violence if they refuse to pay.

"Extortion is a touchy subject," Andrews said, "because it often deals with intimate or very personal information. Army personnel, however, need to be upfront and report it, and they should not pay any money if they are being extorted."

CID officials said the best thing Soldiers, civilians, and their family members can do is to try to prevent it from ever taking place. All are encouraged to be cautious with their online presence and what information they give to people they have met online or via email, and be vigilant when receiving calls from individuals posing as legitimate businesses.

Whether or not your data has been stolen, officials said, you need to be informed and wary of spam, phishing emails and promises of protection by identity theft and credit repair services from future exposure. Officials further warn individuals to be suspicious of communications regarding data breaches that do not come from credible sources.

If you receive a phone call or email you believe to be an extortion attempt, take the following measures:

- If the safety or wellbeing of someone is in imminent danger, contact local law enforcement immediately

- Do not reply to the email, click on any links, or open any attachments
- Report the email to the Internet Crime Complaint Center at www.ic3.gov
- File a complaint with the Federal Trade Commission at www.ftccomplaintassistant.gov
- Report the email to your email and Internet service provider
- Move the email to your SPAM folder
- If contacted through social media, report the contact to the social media provider

"The CID will continue to aggressively investigate and work with our global partners to prosecute those who threaten our military forces and attempt to defraud them of their hard-earned money," Andrews said.

Soldiers, Army civilians, and their family members who have been threatened with extortion should contact their installation Military Police or CID office. Individuals can also email CID at Army.CID.Crime.Tips@mail.mil, or call 1-844-ARMY-CID (844-276-9243).

-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 cybercrime 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.