United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

CID Lookout
On Point for the Army

Cybercriminals targeting USAA members

QUANTICO, Va., February 6, 2015 – Recent crime reports reveal a social media fraud scheme targeting United Services Automobile Association (USAA) members. The scheme may target other groups or financial institutions because the techniques can be easily adapted. With this in mind, special agents with the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) are strongly recommending that anyone with a USAA account be wary if receiving communication on social media from somebody claiming to be associated with USAA or another financial institution.

According to CID agents, the scammer, pretending to be an official representative of USAA, contacts a USAA member on social media (e.g., Facebook, Twitter, Instagram) claiming the member has won an award or is eligible for a customer incentive. In order to receive the award payment, the member is asked to pay a finder's fee, commission or service charge.

Conveniently, the fee can be paid from the proceeds of the award. The scammer asks for the USAA member's mobile banking credentials (username, password, and PIN) and uses USAA's mobile banking application to deposit checks into the member's account. Then, the member is asked to electronically pay the finder's fee to the purported USAA official, usually through a wire or money transfer service like Moneygram or Western Union. Wire and money transfer services are used because traceability is often limited.

Predictably, the deposited award checks are not genuine and, after several days, are returned unpaid and charged back to the USAA member's account. While the deposits are fake, the money the member wires to the scammer is very real.

Most likely, the scammers surf social media content (images and comments) randomly identifying military personnel and their family members. Once identified, they are prime targets for the USAA scam, not because the scammer has specific knowledge of any actual

-more-

USAA affiliation. Rather, the scammers shotgun their messages betting (and current reporting indicates good odds of success) that at least some of the recipients actually have USAA relationships.

CID agents recommend that if you are suspicious about any social media post claiming to be from USAA, you should contact USAA at abuse@usaa.com. For similar scams involving other financial institutions, please contact their security department, the Internet Crime Complaint Center or the United States Federal Trade Commission.

Reminder:
Verify through established channels the authenticity of anyone asking for your personal information, financial information, passwords, PINs and so forth, especially if you did not initiate the interaction.

Recommended Practices:
- Be suspicious when someone you do not know contacts YOU and asks for YOUR personal information.
- Never, in any social media setting, provide usernames and passwords to anyone; your bank will not ask for personal information, including debit card numbers and PINs.
- Verify, verify, verify! Contact the financial institution directly.
- Use a telephone number or email you know to be valid; look on the financial institution's website, the backs of your debit or credit cards or statements.
- DO NOT rely on the person who contacted you to provide a verification telephone number or email. Remember, you are verifying because you are skeptical of the person's reliability.

Additional information about computer safety and cyber related crimes can be found on the U.S. Army Criminal Investigation Command's CCIU webpage at http://www.cid.army.mil/cciu.html. Simply select the Cyber Crimes Advisories on the left side of the page to review previous cyber crime alert notices and prevention flyers.

-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.

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.