



# United States Army Criminal Investigation Command

Media contact:  
571-305-4041

FOR IMMEDIATE RELEASE



## CID: Beware of USAA Telephone Scam

QUANTICO, VA. (Jan. 31, 2019) – The U.S. Army Criminal Investigation Command is warning the Army Community about a recent telephone scam involving USAA.

[According to a press release issued by USAA](#), a scammer will attempt to gain access to an account using deceptive methods via telephone.

A common example is a fraudster spoofing the 800 number and calling members, which means the phone number that shows up for the member appears to be from USAA. The fraudster then impersonates an employee, often a fraud prevention specialist. They gain the member's interest and trust by pretending there are fraudulent charges on the account.

During the conversation, they ask for the member's login information, such as their PIN, password or one-time code to confirm the customer's identity to review the charges. The fraudster then uses the member's information to access their real account during the conversation.

"USAA will never call you and ask for your logon information, which is your PIN, one-time code, password or social security number," said Mike Slaugh, executive director of Enterprise Financial Crime Prevention in the press release.

If you receive an unexpected call from someone asking for your logon information, hang up and contact USAA directly at 1-800-531-USAA.

Additionally, USAA recommends all members use multifactor authentication for an extra layer of security to protect you against fraudsters and cybercrime.

--- CID ---

*For more information on CID, or to report a felony-level crime, provide information concerning a crime, or if you are the victim of a crime, visit [www.cid.army.mil](http://www.cid.army.mil).*