DEPARTMENT OF THE ARMY
U. S. ARMY CRIMINAL INVESTIGATION COMMAND
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134

REPLY TO
ATTENTION OF

Nigerian letter or "419" frauds originated in Nigeria and have grown in popularity with other developing countries as internet access has become available. The scams promise big profits, romance, or solicit assistance in exchange for help moving large sums of money out of a country. Claiming to be foreign officials, business persons, military members, or the surviving spouses of former government leaders, con artists offer to transfer millions of dollars into bank accounts in exchange for a small fee. 419 was the country code for Nigeria. Some utilize photographs obtained from the internet in emails or on social/dating sites to lure unsuspecting citizens into providing money to them for such reasons as transportation costs, communication fees, marriage, processing and medical fees.

Nigerian fraud has been around for decades, but now seems to have reached epidemic proportions. Estimates indicate U.S. Citizens lose approximately 2 billion dollars a year to these scams.

Recently these scams have evolved into Impersonation Fraud affecting our U.S. Service Members. Nigerian personnel in these instances search the internet for photographs of U.S. Service Members, and then utilize these photographs in emails or on social/dating sites to lure unsuspecting citizens into providing money to them for such reasons as transportation costs, communication fees, marriage, processing and medical fees. To date there have been no reports indicating our service members have suffered any financial loss as a result of these attacks. To date, photographs of U.S. Service Members have been the only thing utilized, most of which are readily accessible on the World Wide Web.

The U.S. has established numerous task force organizations to deal with this growing epidemic; unfortunately, the personnel committing these scams are utilizing untraceable email addresses, routing accounts thru 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 and close down their operations is very limited. Unfortunately, as is the situation in most cases, as soon as one incident is resolved, the criminals are finding another means of attack.

In an effort to **protect yourself** from being a potential victim of these scams the following should be considered:

Shred financial documents and paperwork with personal information before you discard them.

Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.

Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with. This includes also, but not limited to, the release of any photographs onto the World Wide Web.
Safeguard your military ID. Keep it with you or locked up at all times.

Never lend your credit cards or account information to anyone else.

Never click on links in unsolicited emails; instead, type in a web address you know. Use security software to protect your computer; keep it up-to-date. If you use Peer-to-Peer file sharing, check the settings to make sure you are not sharing your sensitive private files with other users. These scams almost always start with email, and once your email is identified they will circulate your email address to other personnel conducting another scam.

Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.

Keep your personal information in a secure place, especially if you live in barracks or with roommates.

Don't let mail pile up unattended if you can't collect it. Use a mail stop or P.O. Box, or have someone you trust hold your mail while you are away.

Inspect your credit report and financial statements. Credit reports and financial statements contain information about you, including what accounts you have and your bill-paying history. The law requires each of the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion— provide give you a free copy of your credit report every year if you ask for it. To obtain the free credit report visit www.annualcreditreport.com or call 1-877-322-8228. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Recognizing the need to protect yourself is a good first step in ensuring you do not become a potential victim of these scams. Once your identity has been **compromised,** action needs to be taken to prevent further loss. The following actions should be taken immediately:

Place a "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient as the information will be provided to the other companies. Placing a fraud alert entitles you to free copies of your credit reports also. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

Equifax: 1-800-525-6285
Experian: 1-888-EXPERIAN (397-3742)

TransUnion: 1-800-680-7289

Close accounts. Close any accounts that have been tampered with or established fraudulently.

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 D.C. 20580

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

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

Report the theft to one of your local law enforcement agencies.

FBI: http://www.fbi.gov/homepage.htm
United States Secret Service: http://www.secretservice.gov
United States Postal Inspection Service: https://postalinspectors.uspis.gov

In cases where your identity has been utilized during the commission of these scams (i.e. photograph) with **no further Personally Identifiable Information disclosed**, the following actions should be completed as soon as possible to assist law enforcement:

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

Email: spam@uce.gov

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

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

Report the fraud to one of your local law enforcement agencies.

FBI: http://www.fbi.gov/homepage.htm
United States Secret Service: http://www.secretservice.gov
United States Postal Inspection Service: https://postalinspectors.uspis.gov