

## CREDIT CARD FRAUD

Recently, there have been several reports of external fraudulent activity targeted toward or affecting the government's charge card program.

1. Do not give out account information in response to a fraudulent e-mail indicating it is from Visa officials, stating that cardholders have to "reactivate" their accounts due to a "technical security update." The e-mail directs the user to click a link that appears to be the Visa Web site, but is actually a fake mirror image. Entering personal information into that site could result in identity theft. Note that no one from Visa banks will ever call or e-mail a cardholder and ask for an account number or other personal information. Thus far, this action has been targeted at government travel cardholders. Cardholders should report any attempts to the A/OPC and to the banks (800 number on the back of the credit card) as soon as they occur.

2. Information warns of a potential scam whereas unknown callers falsely identify themselves as bank employees working with the government charge card program. The scam operators claim to be checking suspicious card activity and may ask for account numbers, social security numbers, and other personal information. Be aware that bank employees would not take these actions. The A/OPCs should be the only persons requesting this type of information. Cardholders should report any attempts to the A/OPC and to the banks (800 number on the back of the credit card) as soon as they occur.

If you have any questions on this information, please don't hesitate to contact Leni or myself.