February 2, 2011

PCard-03-2011: Fraud Alert – Visa Validation Phone Scam
FCard-03-2011: Fraud Alert – Visa Validation Phone Scam
TCard-02-2011: Fraud Alert – Visa Validation Phone Scam

This information is being sent by John T. McCain, Program Manager, Charge Card Service Center Program Office.

The CCSC has received notification of a Visa Validation scam being conducted by automated phone calls to cardholders. The particular incident reported involved a call received from an automated service on the cardholder's government-issued cell phone. The automated system attempts to capture charge card information by asking the cardholder to input their card number, expiration, and pin number. Please see the details of the reported incident below.

++

- The fraudulent phone call was received from an automated service on the cardholder's government-issued cell phone.
- The automated system caller's phone number appeared as only 4-digits (1402).
- The automated caller stated that the cardholder's "Visa Debit" card had been invalidated and in order to reactivate it, the cardholder could either call a phone number (1-800-391-8627) or stay on the line. Upon staying on the line, the cardholder was prompted to enter the credit card number, expiration and pin number.
  - Sensing this was a suspicious and possibly fraudulent call, the cardholder **DID NOT** enter any of this information. Instead the cardholder wrote down the number they suggested to call and then called their GSA Customer Service number to report the incident.
  - The GSA Customer Service representative recorded the information and suggested the cardholder alert their supervisor to this fraudulent attempt to gain access to their credit/debit card.

++

***Please immediately inform ALL CARDHOLDERS that these phone calls ARE NOT legitimate Visa messages and should be ignored.** Any reports of this type of activity can be reported to the CCSC at ccsc@dm.usda.gov.

If you receive a phone call or email that appears to be from your card issuer requesting financial information or any other personal data:

- ***Treat the call/email with suspicion.***
- ***Do not give out/enter ANY personal or charge card information over the phone, Internet or mail.***
- ***For emails- Do not reply to the email or respond by clicking on a link within the email message.***
- ***Contact your card issuer as soon as possible to report the suspicious email. Use the number or Web site address on the back of your card or on your monthly statement.***

- ***If you think the request is valid, always contact the bank using the number on the back of your card.***
- ***If anyone ever gives out information, they should immediately call their bank.***

You should be suspicious of any unsolicited phone call that asks for charge card/personal information OR email that asks you to click a link and provide personal or financial information.

Please email any questions to the CCSC at ccsc@dm.usda.gov. Thank you!