General Services Administration

March 9, 2007

GSA SMARTPAY® SMART BULLETIN

U.S. GENERAL SERVICES ADMINISTRATION
FEDERAL ACQUISITION SERVICE
SMART BULLETIN NO. 003

Phone Fraud Scams

INTRODUCTION:

The purpose of this GSA SmartPay® Smart Bulletin is to inform customer agencies of a new type of phone fraud scam involving the Card Verification Value 2 (CVV2) code on the back of charge cards. Although this office cannot confirm any specific incidents of this particular scam involving government cardholders, VISA has confirmed that similar scams exist.

BUSINESS LINE(S) AFFECTED: Purchase, Travel, Fleet, Integrated

SUMMARY:

The GSA SmartPay® Office has been made aware of a new type of phone fraud scam in which criminals who already possess personal information such as names, account numbers, and addresses ask you to verify the 3 digit Card Verification Value 2(CVV2) code on the back of your card. The CVV2 code is often asked for by merchants so that they can secure "card not present" transactions occurring over the Internet, by mail, fax, or over the phone. In many cases, the cardholder is fooled into a false sense of security by the criminal (generally posing as a bank “fraud investigator”) revealing a portion of the cardholder’s personally identifiable information before asking them to “verify” the CVV2 code on the back of their card.

ACTION:

Cardholders should be aware that banks or associations will never ask for personal information via phone or email unless the call was initiated by the cardholder. Never reveal any personal information when solicited via phone or email. Instead, if unsure, contact the bank or association directly using a phone number or email address you know is valid, to confirm that you are speaking with an authorized employee. Never use any phone numbers or hyperlinks provided to you in unsolicited phone calls or emails. Instead, use the phone numbers provided on the back of your card, or manually enter a

url that you know to be official into a separate browser (i.e. close the website in question and re-open a web browser such as Internet Explorer, Netscape, or Firefox to enter a url address that you know to be authentic).

For more information on how to protect your self against common scams, fraud and identity theft, please visit the following association links:

http://usa.visa.com/personal/security/protect_yourself/common_frauds/index.html

http://www.mastercard.com/us/personal/en/securityandbasics/fraudprevention/index.html

Bertha Gelhaus
Contracting Officer, GSA SmartPay®

David J. Shea
Director, GSA SmartPay®

If you have any questions or comments regarding this Smart Bulletin, please contact Bertha Gelhaus at 703-605-2865 or bertha.gelhaus@gsa.gov.

[END]