WASHINGTON HEADQUARTERS SERVICES
BUDGET AND FINANCE DIRECTORATE

PURCHASE CARD ALERT NUMBER 18

(Issue date: 30 January 2004)
THIS ALERT IS APPLICABLE TO:

APPROVING OFFICIALS	X
CARDHOLDERS	X

SUBJECT: Security Alert – Fraudulent E-mails and Telephone Scams

The purpose of this Purchase Card Alert is threefold:

1) To notify Approving Officials and Cardholders that there are recent reports of numerous scam artists employing devious means to obtain purchase card account information;
2) To provide examples of possible methods used by scam artists to obtain the account information and;
3) To advise account holders to report any such requests for information to US Bank and the APC.

US Bank issued a security alert regarding fraudulent e-mails. The bank alert is presented in its entirety under Item Number 1 -- "Fraudulent E-Mails", below. Please read and heed the contents of the US Bank alert.

Item Number 2 – "Example of Possible Telephone Scam" depicts one method that may be used by individuals with criminal intent to glean account information from unsuspecting account holders. We've been unable to verify the legitimacy of this report, but in an effort to increase vigilance, it is being disseminated as an example of one type of scam that may be employed.

Bottom line: Neither US Bank nor Visa will ever contact cardholders directly under any circumstances to verify account numbers or personal information. Criminals are getting increasingly more devious and cunning, so cardholders and approving officials must be very cautious. You must be on alert for this type of activity and safeguard your account number at all times.

IF YOU RECEIVE A REQUEST FOR ACCOUNT INFORMATION, IMMEDIATELY REPORT IT TO US BANK AND TO THE APC.

ITEM NUMBER 1 - FRAUDULENT E-MAILS

To: Card Program Administrators
From: U.S. Bank Corporate Payment Systems
Re: SECURITY ALERT – FRAUDULENT CARDHOLDER EMAILS

We have had reports from cardholders that they are receiving requests via email that appear to come from U.S. Bank. The email claims that the recipient's accounts have been blocked and asks the recipient to enter his or her account number and other personal information.

According to U.S. Bank's Fraud Prevention and Investigation area, this is a fraudulent email and did not come from U.S. Bank. Their instructions to recipients are DO NOT REPLY to this email under any circumstances and furthermore, do not click on the link in this email.

U.S. Bank will not contact cardholders directly under any circumstances to verify account numbers or personal information. This is an excellent time to remind cardholders that if they ever receive a request like this via email or telephone, they should not respond.

We would also like to assure all clients that there has been no fraudulent activity reported and no cards have been suspended as this email suggests. There was no breach of any secure account information. These emails are random and are being sent using a spam list that includes individuals who in many cases do not even have U.S. Bank accounts. Similar email fraud campaigns have been reported using names of other banks, too.

Reporting Fraudulent Email

U.S. Bank and the Federal Bureau of Investigation (FBI) are working diligently to stop these illegal activities. To help track these cyber-criminals, the U.S. Bank Fraud Department is requesting that anyone who has received a suspicious email send a copy of it to fraud_help@usbank.com, along with their responses to the questions below.

- Do you have an account relationship with U.S. Bank?
- What Internet Service Provider (ISP) do you use?
- What type of connection do you use to access the Internet? Cable, dialup, DSL or other?
- Do you have a firewall installed on your computer?

ITEM NUMBER 2 – EXAMPLE OF POSSIBLE TELEPHONE SCAM

The person calling says, "This is Carl Patterson (any name) and I'm calling from the Security and Fraud department at VISA. My Badge number is 12460.

Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card issued by 5/3 bank. Did you purchase an Anti-Telemarketing Device for$497.99 from a marketing company based in Arizona?"

When you say "No".

The caller continues with, "Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards.

Before your next statement, the credit will be sent to (THEN GIVES YOU YOUR ADDRESS)), is that correct?"

You say, "Yes".

The caller continues..."I will be starting a fraud investigation. If you have any questions, you should call the 800 number listed on your card 1-800-VISA and ask for Security.

You will need to refer to this Control #". (THEN GIVES YOU A 6 DIGIT
NUMBER) "Do you need me to read it again?"
Caller then says he "needs to verify you are in possession of your card. TURN THE CARD OVER ...
THERE ARE 7 NUMBERS: FIRST 4 ARE (any 4 numbers are

read) the NEXT 3 are the security numbers that verify you are in possession of the card.

"THESE ARE THE NUMBERS YOU USE TO MAKE AN INTERNET PURCHASE TO PROVE YOU HAVE THE CARD. READ ME THE 3 NUMBERS!"

Then he says "That is correct. I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions? Don't hesitate to call back if you do."

You actually say very little, and they never ask for or tell you the card number.

But after we were called on Wednesday... we called THE NUMBER ON THE BACK OF THE CARD within 20 minutes to ask a question. Are we glad we did!

The REAL VISA security dept. told us it was a scam and in the last 15 minutes a new purchase of $497.99 WAS PUT ON MY CARD!

Long story made short...
We made a real fraud report and closed the VISA card and they are reissuing as a new number.

WHAT THE SCAM WANTS IS THE 3 DIGIT NUMBER!!!! and that once the charge goes through, they keep charging every few days.

By the time you get your statement, you think the credit is coming, and then it’s harder to actually file a fraud report.

THE REAL VISA REINFORCED THAT THEY WILL NEVER ASK FOR ANYTHING ON THE CARD THEY ALREADY KNOW!!

What makes this more remarkable is that on Thursday, I got a call from "Jason Richardson of MasterCard" with a word for word repeat of the VISA Scam.

This time I didn't let him finish. I hung up. We filed a police report (as instructed by VISA), and they said they are taking several of these reports daily !!

If you have questions regarding this Purchase Card Alert, or anything else under the OSD/WHS Purchase Card Program, please don't hesitate to contact an APC. The APC's are Ms. Tracy Williams (twilliams@bfd.whs.mil) on 703-695-6343 or Mrs. Claudia Colvin (ccolvin@bfd.whs.mil) on 703-614-5382.

You can access valuable information regarding the Purchase Card Program on our web page at:

http://www.bfd.whs.mil/referencelib/cardholders/PCP.htm