NUREG/BR-0304

Volume 1, Number 2
November 2003

UNITED STATES NUCLEAR REGULATORY COMMISSION

OIG Information Digest

Good, Bad, and "Fare" Travel

This edition of the *OIG Information Digest* highlights topics pertaining to Government travel that can have a positive or negative effect on an NRC employee depending on whether Government guidelines are followed.

NRC travel procedures and guidelines have greatly changed over the past 10 years in response to the traveling needs of the Government employee. Per diem rates have increased in an effort to keep pace with the cost of travel. Federal employees are now entitled to receive certain travel benefits that, in the past, were prohibited.

Federal Travel Regulation: Using Promotional Materials and Frequent Traveler Programs

On December 28, 2001, President Bush signed into law a provision that Federal employees may retain promotional items such as frequent flyer miles and travel upgrades for personal use. The final rule was effective April 12, 2002. The General Services Administration (GSA) is issuing regulations allowing Federal employees to retain and make personal use of promotional items earned while on official Government travel. A Federal traveler who receives a promotional item such as frequent flyer miles, upgrades to business or first class, or access to carrier clubs or facilities as a result of using travel or transportation services obtained at Federal Government expense may retain the promotional item for personal use if it is obtained under the same terms as those offered to the general public and at no additional cost to the Federal Government.

This final rule amended the Federal Travel Regulation (FTR) by removing provisions requiring that promotional benefits, including frequent flyer miles earned on official travel, be considered Government property only to be used for official travel.

Since frequent traveler benefits may now be retained for personal use, you may use any frequent traveler benefits you have earned to upgrade your transportation class to business or first class service and for personal air travel. No approval is necessary for this upgrade because redeeming your own frequent flyer miles for an upgrade is equal to using your own personal money. NRC Management Directive 14.1 will be revised in the near future to reflect all these changes. In the meantime, Network Announcements will be provided to all NRC employees with updates and new rules concerning travel guidelines.

Inside this issue:

Special points of interest:

- *OIG Investigations on Use of Travel Card*
- *OIG Investigations on the Full Share Program*
- *Audit of Personnel Security Program*
- *Audit of Protection of Safeguards Information*

Good, Bad, and "Fare" Travel (cont. from page 1)

OIG Investigations on Personal Use of Travel Card

OIG continues to receive indications of NRC employee misuse of the Government VISA travel card which in certain cases leads to an investigation. The following are summaries of those investigations:

One OIG investigation determined that 30 personal purchases were made on an NRC employee's Citibank Government VISA travel card totaling over $2,500. These purchases were not made in connection with any official Government travel and included charges for personal airline tickets, entertainment, medical treatment, gasoline for personal vehicles, and other miscellaneous expenses.

Another OIG investigation disclosed that an NRC employee submitted a fraudulent temporary quarters contract to the Travel Office to obtain $1,400 in reimbursement from the Government for compensation that was improperly paid. This employee also used the NRC Citibank VISA card for cash withdrawals totaling over $4,000. This employee was terminated from Federal service.

Another OIG investigation determined that an NRC employee made 58 personal purchases on the employee's NRC Citibank Government VISA travel card which totaled over $10,000. These personal purchases were not made in connection with any official NRC business and, according to NRC travel records, the employee had not traveled on official NRC business for 5 years. This employee was terminated from the NRC.

NRC's Full Share Program (MD 13.4 Part III)

Management Directive 13.4, Part III, states that as a result of the Federal Employees Clean Air Incentives Act of 1994, executive departments and independent agencies may participate in any program established by a State or local government that encourages employees to use public transportation. In accordance with this authority, NRC provides employee public transportation subsidies subject to budget limitations and the local transportation environment.

In December 1991, NRC started the Full Share Program by providing eligible employees with a subsidy of up to $21 per month. That subsidy has now increased to a maximum of $100 per month. At headquarters, this subsidy is provided in the form of a Metrochek, a fare voucher that looks and works like a Metrorail farecard. Metrocheks can either be used as a metrorail farecard or redeemed for other transit media (e.g., Metrobus, Ride-On, or MARC rail).

NRC headquarters employees wishing to participate in the Full Share Program must register with the Administrative Services Center (ASC) and certify that Metrocheks received under the program will be used **solely to commute to and from work.**

The ASC also provides order forms to redeem a Metrochek for the other fare media discussed above. Employees may redeem Metrocheks for any of these fare media at the Montgomery County Transportation Office. Metrochek brochures providing additional information on this program are available in the ASC. For more detailed information about the Full Share Program, log onto www.wmata.com.

Regions II and III have subsidy programs similar to the headquarters program. Employees may participate in these programs by completing an application form provided by their Division of Resource Management and Administration. At this time, Region I does not have a subsidy program in place because its offices are not accessible via public transportation. Region IV provides a subsidy to employees who participate in van pools.

Employees who qualify for the Full Share Program are given a monthly transit benefit with a subsidy not to exceed $100. Each employee must fill out an application stating their home address, mode of transportation, and the mileage and cost associated with their commute. Each

Good, Bad, and "Fare" Travel (cont. from page 2)

applicant is required to sign the following certification:

I hereby acknowledge receipt of the Metrochek as a monthly transportation fringe benefit valued at $$ (total) per month.

This monthly benefit does not exceed my average monthly commuting cost based on a 20-day month commute by public transportation or eligible vanpool.

I certify that I will use the fare media purchased under this program exclusively for my regular daily direct commute from home to work and return. I will not give, barter, exchange, convey, or otherwise transfer this benefit to any other person. I understand and agree that false certification may result in disciplinary action taken by my employer up to and including dismissal from employment and possible prosecution for Federal income tax evasion.

OIG Investigations Concerning Employee Use of the Full Share Program

OIG conducted a review of the NRC Full Share Program to identify potential deficiencies in the administration of the program.

As a result of these investigations, OIG found that one NRC employee deliberately misused the program subsidy by giving the subsidy totaling $1,075.90 to a personal friend, and another NRC employee falsely certified two applications for the program when the employee listed a home address that was not used in the daily commute between home and work. This NRC employee inappropriately received $2,522 in transportation benefits.

A third NRC employee, who claimed to reside in Washington, DC when, in fact, the employee resided in Rockville, MD inappropriately received $905 in benefits. This employee also misused the subsidy program by using the Full Share Program farecard for personal travel. NRC recovered the farecards whose value totaled $2,522.

OIG Audits

Ongoing Audits

Audit of NRC's Personnel Security Program

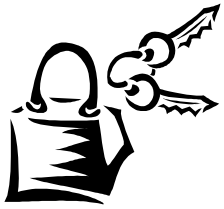
NRC's Personnel Security Program makes determinations on the initial and continuing eligibility of NRC applicants, consultants, and employees for facility access authorizations, employment clearances, and access to restricted data and national security information. The program also makes determinations on the initial and continuing eligibility of contractor employees for building access and for access to sensitive information technology systems and data. This audit continues audit work performed during FY 2003 on this issue. In FY 2003, auditors focused on the personnel security process as it pertains to contractor employees. During FY 2004, auditors are focusing on other program components to determine whether the program is effectively managed and achieves its goals.

Audit of NRC's Protection of Safeguards Information

Safeguards information is sensitive unclassified information that specifically identifies the detailed (1) security measures of a licensee or an applicant for the physical protection of special nuclear materials or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. NRC established its Sensitive Unclassified Information Security Program to ensure that sensitive unclassified information is handled appropriately and is protected from unauthorized disclosure under

OIG Audits (cont. from page 3)

pertinent laws, management directives, and applicable directives of other Federal agencies and organizations. This audit is assessing whether NRC's program (1) adequately ensures the protection of safeguards information, (2) prevents the inappropriate release of safeguards information to the public and NRC employees who should not have access, and (3) adequately defines what constitutes safeguards information.



Identity Theft

The problems associated with identity theft cannot be overemphasized. Identity theft is becoming more and more prevalent with the ease and access of using ATM cards (debit cards) at most stores and credit cards over the Internet. Daily radio broadcasts describe the numerous ways in which members of the public can be victimized by identity theft scams. OIG has published two bulletins describing measures to help you avoid falling victim and steps to take if you become a victim. Copies of this bulletin can be accessed by going to the NRC Web site and clicking on Inspector General, OIG Publications, and Fraud Bulletins/Information Digest. The April 2003 bulletin deals primarily with identity theft. This bulletin can be downloaded and printed.

Online Auctions Dominate Consumer Fraud (Article from the National Consumer's League)

Last year, the National Consumer's League received a record number of complaints about online scams, with complaints about online auctions rising dramatically. In 2002, 36,802 complaints were filed about online scams, more than twice the 15,864 complaints received in 2001. Ninety percent of the complaints during 2002 pertained to online auctions, compared to 70 percent in 2001. The other top complaints pertained to general merchandise sales, Nigerian money offers, computer equipment and software, and Internet access services.

Most auction bidders are looking for bargains, hard-to-find items, or things they collect. The average purchase is $100 or less, but some people spend much more. Many buyers pay by sending a personal check, cashier's check, or money order directly to the seller. Below is some advice for online auction bidders:

Check the seller's feedback rating if that information is available on the auction site. While a positive rating is no guarantee that you won't have a problem, a negative rating is a danger sign. On one of the most popular auction sites is a column called Seller Information and a link to feedback reviews that allow the consumer to read responses from other consumers regarding satisfaction with the product and response from the seller. Be sure to read all the comments before you place your bid.

Look for information about insurance and understand the terms. Some auction sites offer insurance protection, but coverage is limited to set amounts, there is usually a deductible, and there may be exclusions; for example, you may not be able to make a claim if you purchase something from a seller whose feedback rating was negative at the time of sale.

Pay the safest way. If you pay the seller directly with a credit card, you can dispute the charges if the item never arrives or was misrepresented. You don't have that right if you use a third-party online payment service, even if you use your credit card to put the money into your account with the service. However, your credit card issuer may still be willing to help you.

Identity Thief Goes "Phishing" for Consumers' Credit Information

An identity thief who allegedly used hijacked corporate logos and deceptive spam to con consumers out of credit card numbers and other financial data has agreed to settle Federal Trade Commission (FTC) charges that his scam violated federal laws. If approved by the court, the defendant, a minor, will be barred for life from sending spam and will give up his ill-gotten gains.

The FTC alleged that the scam, called "phishing," worked like this: Posing as a representative of America Online (AOL), the con artist sent consumers e-mail messages claiming that there had been a problem with the billing of their AOL account. The e-mail warned consumers that if they didn't update their billing information, they risked losing their AOL accounts and Internet access. The message directed consumers to click on a hyperlink in the body of the e-mail to connect to the "AOL Billing Center." When consumers clicked on the link they landed on a site that contained AOL's logo, AOL's type style, AOL's colors, and links to real AOL Web pages. It appeared to be AOL's Billing Center. But it wasn't. The defendant had hijacked AOL's identity and was going to use it to steal consumers' identities as well, the FTC alleged.

The defendant's AOL lookalike Web page directed consumers to enter the numbers from the credit card they had used to charge their AOL account. It then asked consumers to enter numbers from a new card to correct the problem. It also asked for consumers' names, mothers' maiden names, billing addresses, social security numbers, bank routing numbers, credit limits, personal identification numbers, and AOL screen names and passwords - the kind of data that would help the defendant plunder consumers' credit and debit card accounts and assume their identity online.

According to the FTC, the defendant used the information to charge online purchases and open accounts with PayPal. In addition, he used consumers' names and passwords to log on to AOL in their names and send more spam. Finally, he recruited others to participate in the scheme by convincing them to receive fraudulently obtained merchandise he had ordered for himself.

The agency charged the defendant's practices were deceptive and unfair, in violation of the FTC Act. In addition, the FTC alleged that the defendant's practices violated provisions of the Gramm-Leach-Bliley Act designed to protect the privacy of consumers' sensitive financial information.

"Phishing is a two-time scam," said Timothy J. Muris, Chairman. "Phishers" first steal a company's identity and then use it to victimize consumers by stealing their credit identities. This is the FTC's first law enforcement action targeting phishing. It won't be the last," he said. The settlement would bar the defendant from future violations of the FTC Act and the Gramm-Leach-Bliley Act. It also would bar the defendant from sending spam in the future. In addition, the order would require the defendant to give up $3,500 in ill-gotten gains.

An FTC Consumer Alert, "How Not to Get Hooked by a 'Phishing' Scam" warns consumers who receive e-mail that claims an account will be shut down unless they reconfirm their billing information not to reply or click on the link in the e-mail. Consumers should contact the company that supposedly sent the message using a telephone number or Web site address they know to be genuine.

More tips to avoid phishing scams can be found at http://www.ftc.gov/bcp/conline/edcams/spam/coninfo.htm.

To file a complaint or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1 877-382-4357), or use the complaint form at http://www.ftc.gov. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Identity Thief... (cont. from page 5)

If you receive unwanted spam e-mail you can report it to the Federal Trade Commission. Send a copy of any unwanted or deceptive messages to uce@ftc.gov. If you want to complain about a removal link that doesn't work or not being able to unsubscribe from a list, you can fill out the FTC's online complaint form at www.ftc.gov.

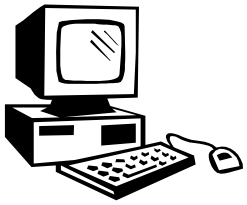
Your complaint will be added to the FTC's Consumer Sentinel database and made available to hundreds of law enforcement and consumer protection agencies. Whenever you complain about spam, it's important to include the full e-mail header. Send a copy of the spam to your ISP's abuse desk. By doing this, you can let the ISP know about the spam problem on their system and help them stop it in the future. Complain to the sender's ISP. Most ISPs want to cut off spammers who abuse their system.

Steps to Computer Security (Article from the National Consumer's League)

Pick an effective password using numbers and characters. Avoid using obvious things such as your birth date or your children's or pets' names.

◊ Build a firewall. A firewall is like the fence around a fort. It makes it hard for intruders to get into your computer from cyberspace.

◊ Take extra security precautions when you have broadband Internet access. Broadband services, which provide consumers with faster access to the Internet, are increasingly available through telephone companies, cable companies, and by satellite. If you have broadband service, you're always connected to the Internet when your computer is turned on. When you're connected to the Internet through broadband service, you are more vulnerable to hackers who may try to get financial and other personal information that is stored on your computer.



◊ If you are not using your computer for extended periods of time, make sure you turn it off. A hacker cannot access a computer that is not on.

We're on the Web! Click on the NRC Public Web site and then the link to the Inspector General. Follow that link to the OIG Hotline and then click on the On-line form.

Organization

UNITED STATES NUCLEAR REGULATORY COMMISSION

11545 Rockville Pike
Mail Stop T 5D28
Rockville, MD 20851

Hotline Number 800-233-3497
Fax: 301-415-5091

Office of the Inspector General