OIG INFORMATION DIGEST

United States Nuclear Regulatory Commission
NUREG/BR-0304

THEFT IN NRC OFFICE SPACE

Volume 3, No. 1

March 2005

Inside this issue:

Special points of interest:

- *Protect Your Valuables in the Work Place*
- *Maintain Vigilance Over Non-NRC Employees*
- *More on Identity Theft*

On August 16, 2004, between 11:30 a.m. and 11:47 a.m., a female posing as an NRC employee gained unauthorized entry to NRC headquarters and wandered through the One White Flint North and Two White Flint North buildings taking cash from unattended cubicles and offices. The subject's entry into the NRC buildings took place during a "Code Orange" alert day.

The OIG investigation identified the subject and, subsequent to her apprehension, she agreed to cooperate with OIG. She was interviewed to determine how she gained entry to the NRC headquarters buildings and how she was able to move freely once inside the buildings.

As a result of this interview, OIG learned of the following sequence of events that allowed a non-NRC employee to enter NRC headquarters and commit theft.

<u>Security Awareness and Vigilance by NRC Staff</u>

According to the subject, she entered NRC property from the street and walked behind One White Flint North to the door located on the Two White Flint North side of the connector between the two headquarters buildings. There she pretended to be an NRC employee on a cigarette break. She waved to two NRC employees walking on the inside of the connector and indicated her desire to enter the building. Two unidentified NRC employees unlocked the door and, without an identification check, allowed her to enter the connector. As part of her impersonation, the subject was wearing a badge on her collar. A cursory examination of the badge by the NRC employees would have revealed that it was not and did not resemble an NRC badge.

<u>Interior Security Identification Vigilance</u>

According to the subject, once inside the NRC buildings, she easily passed through secured card-keyed doors by following NRC employees who opened the doors with their identification badges. In each of these instances, the employees opened the doors, allowed her to enter behind them, and did not challenge her identification. Additionally, although she was confronted by several NRC employees who questioned her presence in two different offices, these employees did not ask her name or examine the badge she displayed on her collar.

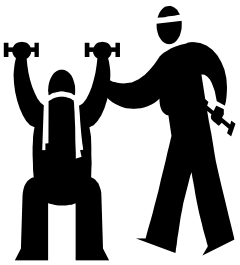
THEFT IN NRC OFFICE SPACE (cont. from page 1)

Security Reminders for Employees

It is the duty of every NRC employee to challenge unfamiliar individuals trying to access NRC office space if those individuals do not have an appropriate badge or their badge is not visible. Do not allow anyone to "piggy-back" on your ID badge unless you recognize them. If you do not want to confront anyone, use the nearest telephone to contact the One White Flint North guard desk at 415-2069 or the Two White Flint North guard desk at 415-5702 for assistance. In this day of elevated security, it is always wise to err on the inquisitive side rather than allow a security breach that could result in harm to

MISUSED CREDIT CARD SCENARIOS

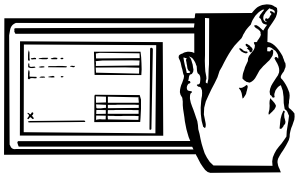
individuals or the compromise of sensitive or classified information. Everyone today knows about the dangers of identity theft. We read about it in the newspaper, and we learn about it from the radio and from television. It is all very real and true and it can happen to anyone. Here are a few more examples of how your identity can be stolen.



1. A friend went to the local gym and placed his belongings in the locker. After his workout and a shower, he came out, saw the locker open, and thought to himself, "Funny, I thought I locked the locker. " He dressed and just flipped the wallet to make sure all was in order. Everything looked okay - all cards were in place.

A few weeks later his credit card bill came - a whopping bill of $14,000! He called the credit card company and started yelling at them, saying that he did not make the transactions. Customer care personnel verified that there was no mistake in the system and asked if his card had been stolen. "No," he said, but then took out his wallet, pulled out the credit card, and - you guessed it - a switch had been made. An expired similar credit card from the same bank was in the wallet. The thief broke into his locker at the gym and switched cards.

Verdict: The credit card issuer said since the victim did not report the card missing earlier, he would have to pay the amount owed to them. How much was he told he would have to pay for items he did not buy? He was told $9,000! But, according to the law, consumers are only responsible for $50! Why were no calls made to verify the amount charged? Small amounts rarely trigger a "warning bell" with some credit card companies. It just so happens that all the small amounts added up to one big one!



2. A customer at a local restaurant paid for his meal with his credit card. The bill for the meal came, he signed it, and the waitress folded the receipt and passed the credit card along. Usually, he would just take it and place it in his wallet or pocket. This time, however, he actually took a look at the card and, lo and behold, it was the expired card of another person.

He called the waitress and she looked perplexed. She took it back, apologized, and hurried back to the counter under the customer's watchful eye. All the waitress did while walking to the counter was wave the wrong expired card to the counter cashier, and the counter cashier immediately looked down and took out the real card. No exchange of words -- nothing! She took it and came back to the man with an apology.

Verdict: Make sure the credit cards in your wallet are yours. Check the name on the card every time you sign for something and/or the card is taken away for even a short pe-

MISUSED CREDIT CARD SCENARIOS (cont. from page 2)

riod of time. Many people just take back the credit card without even looking at it, thinking that it has to be theirs.

For your own peace of mind, develop the habit of checking your credit card each time it is returned to you after a transaction!

3. Yesterday a customer went into a pizza restaurant to pick up an order that he had called in. He paid by using his Visa Check Card which, of course, is linked directly to his checking account. The young man behind the counter took his card, swiped it, then laid it flat on the counter as he waited for the approval, which is pretty standard procedure.

While the customer waited, the young man picked up his cell phone and started dialing. The customer noticed the phone because it is the same model he has, but nothing seemed out of the ordinary. Then he heard a click that sounded like his phone sounds when he takes a picture. The young man then gave him back his card but kept the phone in his hand as if he was still pressing buttons.

Meanwhile, the customer was thinking…"I wonder what he is taking a picture of," oblivious to what was really going on. It then dawned on him. The only thing there was his credit card, so now the customer paid close attention to what the young man was doing. He set his phone on the counter, leaving it open. About five seconds later, the customer heard the chime that tells you that the picture has been saved. Now the customer was standing there struggling with the fact that this boy just took a picture of his credit card. Yes, he played it off well, because had they not had the same kind of phone, the customer probably would never have known what happened. Needless to say, the customer immediately canceled his card as he was walking out of the pizza parlor. Be aware of your surroundings at all times. Whenever you are using your credit cards, take caution and don't be careless. Notice who is standing near you and what they are doing when you use your card. Be aware of cell phones because many have a camera feature these days.

Verdict: When you are in a restaurant and the waiter/waitress brings your card and receipt for you to sign, make sure you scratch the number off. Some restaurants are using only the last four digits, but a lot of them are still putting the whole thing on there. Anyone who has been a victim of credit card fraud knows it is not fun. The truth is that they can get you even when you are careful, but don't make it easy for them.

Mailbox Theft

Another way thieves can steal your identity is by taking mail from your mailbox. In one neighborhood, a thief who stole someone's mail hit about 200 other people in that same neighborhood.

He used a stolen credit card to buy a new computer and made a spreadsheet to log Social Security numbers, bank accounts, and other personal information he got from their mail. Stealing mail to assume someone's identity is big business anytime, anywhere in the U.S., but tax season can be especially fruitful as W-2 forms and other sensitive information containing bank and Social Security numbers arrive in mailboxes.

Thieves today are not the same as they were 5 or 10 years ago. They have become very sophisticated at mining pieces of information to assume the identities of others. It's this type of sensitive data that enables scammers to take full advantage of other mail they steal from you–namely those unsolicited direct mail applications for pre-approved credit cards, loans, or refinancing opportunities which have increased by 5 billion pieces since the National Do Not Call Registry went into effect in October 2003. Some individuals will even go to extreme measures to steal your identity by rifling through your trash. Some identity thieves follow

United States Nuclear Regulatory Commission
NUREG/BR-0304

HOTLINE NUMBER
1-800-233-3497

TDD LINE
1-800-270-2787

USNRC
Office of the Inspector General
11545 Rockville Pike
Mail Stop T 5D28
Rockville, MD 20852

Phone: 301-415-5930
Fax: 301-415-5091

WE'RE ON THE WEB! GO TO THE NRC WEBSITE, CLICK ON INSPECTOR GENERAL, CLICK ON HOTLINE, AND THEN CLICK ON THE ON-LINE FORM AND FILL OUT YOUR COMPLAINT.

MISUSED CREDIT CARD SCENARIOS (cont. from page 3)

mail trucks to steal the delivered incoming mail. With your Social Security or bank account numbers from some pieces of stolen mail, they just complete the applications to get a credit card in your name.

In about 15 minutes, you can stop receiving much of the most shred-worthy mailings:

- Call (888) 567-8688 to remove your name from lists sold to credit card companies by consumer reporting firms such as Equifax and Experian.

- Stop solicitations from the Direct Marketing Association's 5,200 member companies, which represent 80 percent of these marketers. Get forms for $5 at www.dmaconsumers.org/cgi/offmailinglist. Or write for free forms to the Direct Marketing Association, Mail Preference Service, P.O. Box 643, Carmel, NY 01512.
- Remove yourself from some mortgage refinancing and home equity loan offers by calling the Acxiom U.S. Consumer Hotline at (877) 774-2094 or writing to DataQuick, Attn: Opt-out Department, 9620 Towne Center Drive, San Diego, CA 92121.

IDENTITY THEFT (Source: Federal Trade Commission)

Identity theft is the number one consumer complaint in a new Federal Trade Commission (FTC) report. The FTC on Tuesday, February 1, released its annual report detailing consumer complaints filed with the FTC in 2004. For the fifth year in a row, identity theft topped the list of complaints, accounting for 39 percent of the 635,173 consumer fraud complaints filed with the agency last year. Credit card fraud was the most common form of reported identity theft, followed by phone or utilities fraud, bank fraud, and employment fraud. The major metropolitan areas with the highest per-capita rates of reported identity theft were Phoenix, Mesa, and Scottsdale, AZ; Riverside, San Bernardino, and Ontario, CA; and Las Vegas, and Paradise, NV.