UNITED STATES NUCLEAR REGULATORY COMMISSION

June 2007

NUREG/BR-0304 Volume 4, Number 1

OIG Information Digest

Identity Theft

The Office of the Inspector General (OIG) first published information on Identity Theft in March 2000 and again in April 2003. In the four years since the last publication, this country has seen an enormous growth in identity theft and the variety of ways in which a person's identity can be stolen. The individuals that commit this fraud have become very sophisticated and use many tools to steal your identity.

Earlier this year, the OIG received information that Employee Express accounts had been compromised including one for an NRC employee. OIG has also investigated numerous instances where NRC small purchases and travel cards have been compromised. All these instances should warn that identity theft can strike each of us.

In this issue, we will provide you with new information on the different scams and ways to protect yourself and your family in your professional and personal life.

Inside this issue:

Information Regarding Identity Theft (Information from National Consumers League and the Federal Trade Commission)

1. What is Identity Theft?

Identity theft involves someone utilizing your identifying information to acquire goods or services in your name through the use of credit or debit cards, checks, or other documents.

Identity theft is a considerable problem for anyone, but is especially problematic for those people who rely on ATM, credit cards, and other remote access financial services.

2. How Identity Theft Can Happen

Dumpster Diving—Someone rummages through your trash looking for bills or other documents containing personal information.

Skimming—Stealing credit or debit card information by using a special storage device while processing your card.

Phishing—Someone pretends to be from your banking or credit card institution and emails pop-up messages or spam to get you to reveal personal information.

Changing your address—The thief diverts your billing statements to another location by filling out a "change of address" form.

Just Plain Stealing—Someone steals your wallet or purse, mail, pre-approved credit card offers, checks, and income tax information. Sometimes employees steal personnel records from other employees or bribe others who have that information to steal your identity.

3. Detecting Identity Theft

The first line of defense is awareness. Look out for:

- Unusual purchases on your credit cards.
- Being denied a loan for which you qualify.
- Bank statements that do not agree with personal records.
- Unexplained changes in your bank access codes.

Identity Theft (cont. from page 1)

- Unusual calls regarding your personal or financial information.
- Unexplained charges on phone or other consumer accounts.

4. Preventing Identity Theft

- Cut up all credit cards for which you have no use.
- **Shred bank or other financial statements** and any other documents containing personal information such as Social Security Number, date of birth, etc.
- Be creative when you select a password. Don't be obvious by using your phone number, address, birth date, names of children or pets, the last four digits of your Social Security Number, or any format that could easily be decoded by thieves.
- **Destroy pre-approved credit card offers before you throw them out.**
- Make a list of all credit cards, ATM cards, and bank accounts and the phone numbers associated with each, and keep this list in a safe place.

- **Always use secure Web sites for Internet purchases**. You can tell a secure site by the little padlock at the bottom of the page and/or the change at the top of the page from http to either "shttp" or "https."
- Do not discuss financial matters on wireless or cellular phones.
- Write or call the department of motor vehicles to have your personal information protected from disclosure.
- Do not use your mother's maiden name as a password on your credit cards...ask if you can use something else.
- **Be wary of anyone calling or emailing to "confirm" personal information.**
- Thoroughly and promptly review all bank, credit card, and phone statements for unusual activity.
- Monitor when new credit cards, checks, or ATM cards are being mailed to you and report any that are missing or late.
- Remove your Social Security Number from checks
- Do not carry your social security card in your wallet unless needed.
- Order your credit report from Experian, Trans Union, or Equifax (phone numbers are listed on page 6) once a year and look for any anomalies.

5. If victimized, documentation is key.

In the worst cases, identity thieves make enormous unauthorized purchases. By law, once you report the loss, theft, or fraud you have no further responsibility for unauthorized charges. In any event, your maximum liability under Federal law is $50 per card, and most issuers will waive the fee. The bad news is that clearing up your credit records requires significant effort and can take a year or even longer.

By monitoring your personal finances and following the suggestions in this newsletter, you may be able to prevent or minimize losses due to fraud and identity theft. ***It is important to act quickly, effectively, and assertively to minimize the damage.***

6. What to do if you are a victim:

Here are the initial actions victims of identity theft should take to begin the investigative and recovery processes.

Report the crime to your local police immediately. File a detailed police report. Provide as much documented evidence and information as possible. Keep a copy of the incident report and give it to creditors, banks, and merchants who ask for a copy of a police report as part of the fraud investigation.

Call the fraud unit at each of the big three credit bureaus (Equifax, Experian, and Trans Union) to notify them of what has happened. Request copies of your credit reports and ask the bureaus to place a "fraud alert" in your files along with a message asking future creditors to verify by telephone

Identity Theft (cont. from page 2)

any applications added to your report. Follow up with a written letter.

Do not pay any bill or charges that result from identity theft. Contact all creditors immediately with whom your name has been used fraudulently by phone and in writing.

Write a "victim" statement of 100 words or less and send to each of the credit bureaus to include with your credit file.

Get copies of your credit reports monthly following your initial report for at least several months to check for any new fraudulent accounts. The credit bureau should provide these for free.

Call all of your credit card issuers to close your accounts with the notation "account closed at consumer's request" and get new credit cards with new numbers.

Contact your financial institution and request new bank account numbers, ATM cards, and checks. Put stop payments on any outstanding checks that you are unsure of.

Give the bank, credit card, and utility companies a *NEW secret password and PIN numbers* for new accounts. Do not use old PINs, passwords, or your mother's maiden name.

Request a new driver's license with an alternate number from the department of motor vehicles (DMV), and ask that a fraud alert be placed on your old one. Fill out a DMV complaint form to begin the fraud investigation process.

Contact the Social Security Administration and advise them of your situation. Ask them to flag your Social Security Number (SSN) for fraudulent use. Also order a copy of your Earnings and Benefits Statement and check it for accuracy. Changing your SSN is a difficult process and should be used only as a last resort.

Contact the post office and utility companies to ensure that no billing or address changes are made to your account without a written request from you. Request that all changes be verified.

If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport in your name.

Photocopy your driver's license, medical cards, grocery store cards, and all charge cards with their telephone numbers and keep the copies in a safe place in case your wallet is stolen or you are a victim of identity theft.

As appropriate, contact an attorney to help ensure that you are not victimized again while attempting to resolve this fraud. In order to prove your innocence, be prepared to fill out affidavits of forgeries for banks, credit grantors, and recipients of stolen checks.

Be persistent and follow up. Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter.

NOTE: Keep detailed written records of all conversations and actions taken to recover from identity theft. Include names, titles, date/time, phone number, exact circumstances, and action requested. Note time spent and any expenses incurred. Send confirmation correspondence by certified mail (return receipt).

Special Issues Related to Identity Theft

Occasionally, victims of identity theft are wrongfully accused of crimes committed by the imposter or attempts are made to hold them liable for civil judgments. If this occurs, contact the court where any civil judgment was entered and report that you are a victim of identity theft. If you are subjected to criminal charges as a result, quickly provide proof to the prosecutor and investigative agency.

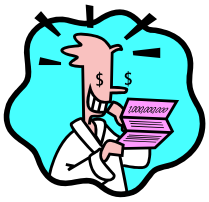
Your credit rating should not be permanently affected, and no legal action should be taken against you as a result of identity theft. If any merchant, financial institution, or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills.

Identity Theft Scams

Watch Out For Scams

Lower credit card rates. With this scheme, someone calls and says they are with your credit card issuer. They say they can lower your interest rate, but they need to have your card's expiration date or part of your account number. HANG UP! Your card issuers already have this information.

Prizes and sweepstakes. A large part of telemarketing fraud complaints are due to phony sweepstakes. In these scams, someone phones or emails to tell you that you've won a prize. You are informed that all you have to do to collect it is send a certified check or provide a credit card number to cover the "cost of processing" your award. Save your money. Legitimate awards do not charge processing fees, in fact, prize offers where you have to pay or make a purchase to be eligible are illegal.



ATM Debit Cards. If your ATM card is lost or stolen, immediately notify your banking institution. If you report the loss or theft within 2 days you will only be liable for $50. If you report the loss or theft after 2 business days but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws. If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days. Check with your own financial institution to find out about their policy.

Recovery Scams. Scammers can purchase lists of those who have been swindled before. They call these people and claim that a victim's lost money can be recovered if he or she pays a fee. Don't buy it. Legitimate law enforcement agencies don't charge to help victims of telemarketing or online fraud.

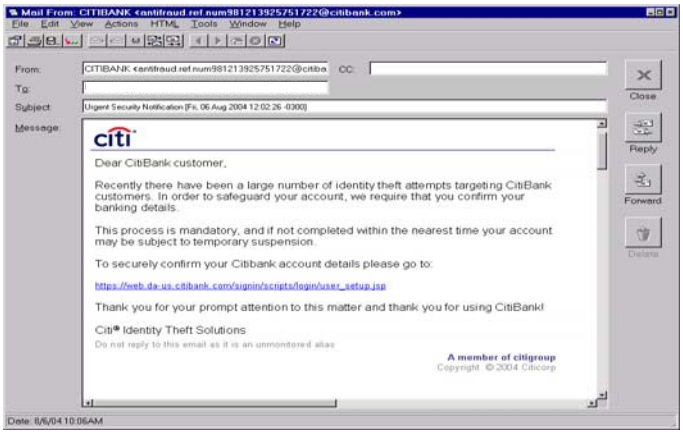
Phishing

Phishing is an email scam that Internet fraudsters use to try and trick consumers into revealing personal information such as debit and credit account numbers, checking account information, Social Security Numbers, or banking account passwords through fake Web sites or in a reply email. The most common form of phishing is by email, although sometimes phishers may contact you by telephone. While you are on your computer, an email may appear from a bank, an internet auction site, or some shopping site that you may have used at one time. This email asks you to validate or update personal information for a phony scheme. They may even threaten drastic consequences if you don't comply. **Don't fall for it**.

How to spot a phishing email

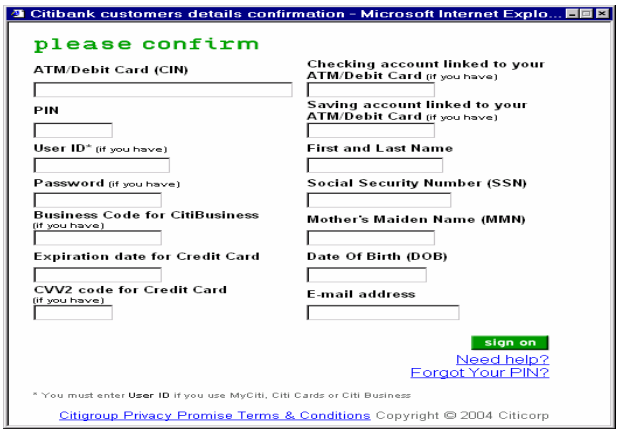
Phishing emails, and the Web site they link to, typically use familiar logos and familiar graphics (as shown in next column) to deceive consumers into thinking the sender or web owner is a government agency or a company they know. Sometimes the phisher urges intended victims to "confirm" account information that has been "stolen" or "lost." Other times the phisher entices victims to reveal personal information by telling them they have won a special prize or earned an exciting reward.

Do not click on a link embedded within any potentially suspicious email, especially if the email requests personal information. If you do, you might



Phishing (cont. from page 4)

be greeted with an official looking form like the following one. If you were to fill this out, you would be



giving an identity thief everything he needs.

<u>Look for these red flags in the email:</u>

- Asks you to provide personal information such as your bank account number, an account password, credit card number, PIN number, mother's maiden name, or Social Security Number.
- Does not address you by your name
- No confirmation of the company that does business with you, such as referencing a partial account number
- Warns that your account will be shut down unless you reconfirm your financial information.
- Warns that you have been a victim of fraud
- Spelling or grammatical errors.

The best way to protect yourself from any scam is the following:

- View any email for financial information or other personal data with suspicion.
- Do not reply to the email and do not respond by clicking on a link within the email message
- Contact the actual business that allegedly sent the email to verify if it is genuine. Call a phone number or visit a Web site that you know to be legitimate, such as those provided on your monthly statements.
- Do not send personal information in response to an email request from anyone or any entity.
- Be cautious. Check your monthly statement to verify all transactions.

The first line of defense is from your Internet Service Provider (ISP). ISP's have a wide variety of tools to identify messages that may be from phishers. These include blacklists from known phishing emails, Web sites, and programs that recognize telltale signs of phishing within the messages. Your ISP can recognize and even keep these phishing emails from ever entering your inbox. Look for information from your ISP about what it is doing to protect you from phishing emails.

Phishing can also occur in other ways. Here is an example of a phishing phone call:

"Is this Mr. Johnson?" I'm calling from XYZ bank. Do you have a Visa card? I need to verify your account because it seems someone may be fraudulently charging purchases to your account. Can you read me the account number and expiration date on the front? OK, now the last four digits on the back…" GOTCHA!!

Here is another one:

"Hello, Charlotte Webb? I represent DKO company and our records show that you have an overdue bill of $500 plus interest and penalties. You don't know anything about this? Well, there could be a mix-up. Is your address 789 Spider Way? What is your Social Security Number?" GOTCHA!

Never give out personal information over the telephone to someone who calls you. Only if **you** initiate the phone call should you provide your personal information.

OIG Cases Involving Identity Theft

Both of the following are actual identity theft incidents which occurred within the past two years and were investigated by the NRC/OIG.

OIG was contacted by an NRC employee who related that she had received a call from an apartment complex manager. The manager was attempting to collect unpaid rent from the employee. However, the employee had never rented an apartment at that complex.

OIG's investigation revealed that another NRC employee had used the first employee's name and identification information to rent an apartment. This employee had a poor credit history and believed an application in her own name would have been turned down. The perpetrator had obtained details about the first employee, including her Social Security Number, from various documents, such as travel vouchers. The victim's supervisor's signature was also falsified on an employment verification form, and was accompanied with a xeroxed copy of her NRC badge that had been altered to contain her picture alongside the first employee's name. Additionally, after failing to pay her rent she used the first employee's name at a DC Landlord and Tenant Court hearing.

OIG coordinated this investigation with the Washington, DC Metropolitan Police. The subject of this investigation admitted to her actions and resigned her position with the NRC. She was also charged in District of Columbia Federal Court, where she pled guilty and was fined and sentenced to 14 months incarceration.

OIG was contacted by an NRC inspector who had found numerous unauthorized charges on her NRC travel card billing statement. The transactions included purchases on Ebay and cell phone charges. The charges totaled over $2,000.

OIG contacted the merchants and obtained details regarding each of the transactions. This investigation ultimately revealed that the inspector had been on official travel shortly before the unauthorized transactions began. The inspector's credit card information, including the verification number on the back, had been copied by a hotel front desk clerk. The clerk, who had previous convictions for forgery and counterfeiting, then used the credit card account number to make purchases on the Internet auction site, Ebay, which she had shipped to her residence. Additionally, the clerk used the credit card number to pay for "ring-tones" and other items downloaded to her personal cell phone.

OIG worked jointly with the Michigan State Police and apprehended the clerk. During an interview, the clerk fully admitted her illegal activities. She subsequently pled guilty and was sentenced to 6 months in jail.

Important Numbers For Your Information

Web Sites to Help You With Identity Theft

Federal Trade Commission
www.ftc.gov
For Identity Theft
www.consumer.gov/idtheft

Banking Agencies

Federal Deposit Insurance Corporation
www.fdic.gov

Federal Reserve System
www.federalreserve.gov

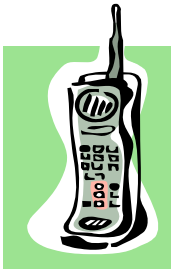
National Credit Union Administration
www.ncua.gov

Office of the Comptroller of the Currency
www.occ.treas.gov

Office of Thrift Supervision
www.ots.treas.gov

Important Numbers to Remember

Social Security Administration Fraud Hotline
1-800-269-0271
To order your Social Security Earnings & Benefits Statement, call
1-800-772-1213



Credit Reporting Bureaus
Equifax: to report fraud
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285
Equifax: to order credit report
1-800-685-1111

Experian: to report fraud and order credit report
1-888-397-3742, www.experian.com

Trans Union: to report fraud
www.transunion.com
1-800-680-7289
Trans Union: to order credit report
1-800-916-8800

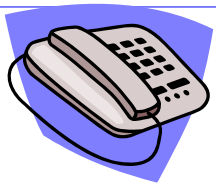
Organization

United States Nuclear Regulatory Commission

Office of the Inspector General
11555 Rockville Pike
Mail Stop T 5D28
Rockville, MD 20852

Hotline Telephone - 800-233-3497

Fax: 301-415-5091



We're on the WEB! Access the HOTLINE Thru the NRC Website!

- Go to www.nrc.gov
- Scroll down to the bottom of the page and click on *Inspector General*
- Click on the phone symbol on the right
- Scroll down to the highlighted area that says *Submit an online form*
- Fill out the form with all pertinent information and click submit