OIG Fraud Bulletin

United States Nuclear Regulatory Commission

NUREG/BR 0272
Volume 4, No. 1
April 2003
OIG Hotline 800-233-3497

Identity Theft

We have all heard about identity theft. Unfortunately, there is a growing concern about how easy it is for someone to steal your identity.

This office first published information on identity theft in our March 2000 issue. However, that issue was not distributed agency wide. We have reprinted that information in this issue to help guide you in the event you become a victim of identity theft.

In this new world of virtual reality, it is important to keep up-to-date on the various scams and how to protect yourself and your family.

We hope this information will prove valuable to you in your professional and personal life.

Inside this issue:

Information Regarding Identity Theft (Information from National Consumers League)

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. 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 don't agree with personal records.
- Unexplained changes in your bank access codes.
- Missing credit card bills or other mail.
- Unusual calls regarding your personal or financial information.
- Unexplained charges on phone or other consumer accounts.

3. ***Preventing Identity Theft***

- Cut up all credit cards for which you have no use. Similarly, when you are finished with them, 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.

Identity Theft (cont. from page 1)

- Destroy pre-approved credit card offers before you throw them out. A home shredder (costs about $20) is the best thing to use to shred financial statements, receipts, and old cancelled checks that you are discarding.

Keep in mind that some of the tips mentioned are quite extreme. You need to use your own judgment if you become a victim of identity theft.

- 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.
- Remove mail promptly from your mailbox. Never use your mailbox for outgoing mail.
- 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.
- Be wary of anyone calling 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.
- Close all unused credit card and bank accounts.
- Remove your social security number from checks, drivers license, or other ID.
- Always ask for the carbon papers from credit purchases.
- 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 4) once a year and look for any anomalies.

4. 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.***

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.

1. *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.

2. ***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 any applications added to your report. Follow up with a written letter.
3. ***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.

Identity Theft (cont. from page 2)

4. ***Write a "victim" statement of 100 words or less*** and send to each of the credit bureaus to include with your credit file.
5. ***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.
6. ***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.

7. ***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.
8. **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.
9. ***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.
10. ***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.
11. ***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.

12. ***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.

13. ***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.
14. ***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).

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.

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.

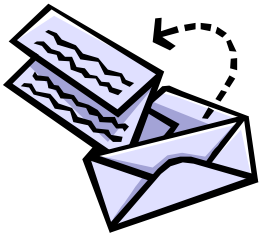
Your credit rating should not be permanently affected, and no legal action should be taken against you as a result of identity theft. If any merchant, financial institution, or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into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

Identity Theft (cont. from page 3)

The stress commonly experienced during identity theft victimization and recovery can be quite severe. Victims should consider counseling assistance as an option for themselves and family members who may be equally traumatized.

Pre-Approved Credit Card Offers

If you don't use credit offers that you receive, dispose of them by shredding. You can avoid getting these offers in the mail by calling a toll-free number operated by the major credit bureaus, 888-567-8688. Your social security number will be requested to identify you. Getting off these marketing lists will not affect your ability to apply for credit in the future.



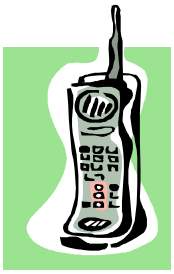
Important Numbers to Remember

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

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

Trans Union to report fraud

1-800-680-7289

Trans Union to order credit report

1-800-916-8800

OIG Investigations on Identity Theft

As the media often reports, credit card fraud is one of the fastest growing identity theft crimes in the United States today. Often, the credit card information is stolen (i.e., compromised) without the card holder's knowledge. This compromise can happen many ways including: compromise through the credit card company files, skimming (making a duplicate of the magnetic strip), and credit card number generating programs. The results can be large dollar losses to the credit card company but can also become a problem for the individual victim. It may take a large amount of time to clear up credit issues and report fraudulent activities to the various agencies. The Office of the Inspector General has investigated a number of these cases. One case involved a retired NRC employee who reported to the OIG that during his retirement process someone may have used his name to fraudulently obtain credit cards.

OIG learned that two banks issued credit cards and cash advances in the retiree's name in the amounts of $9,860 and $9,500. These credit cards were issued to an unknown individual in the name of the retiree.

OIG coordinated this investigation with the United States Postal Service, which is involved in investigating credit card and identity theft fraud.

OIG identified no facts to indicate that the former employee's identity had been compromised by an NRC employee or NRC contractor.

The OIG has also noticed an increase of compromised Citibank Travel cards at the NRC. OIG has investigated several instances of employee Citibank Travel cards that were compromised and used by suspects for large fraudulent retail purchases.

OIG Investigations on Identity Theft (cont. from page 4)

These fraud schemes include the use of counterfeit credit cards that are produced using the information compromised off the NRC employee's credit card. The perpetrators of such crimes know that time is limited with a compromised account and will quickly charge many large ticket items.

In less than a month with only a handful of compromised accounts at the NRC, over $30,000 in fraudulent purchases were documented. Some of the fraud was first identified by Citibank, which then notified the employee. Other fraud was first identified by alert NRC employees who carefully and promptly reviewed their Citibank statements and notified Citibank and OIG. Often, the employee had not even used the card in recent months or had used the card on official travel but still had possession of the original credit card.

A few simple steps can greatly reduce your vulnerability to credit card fraud both on your personal and NRC credit cards:

- Do not take your card with you if you do not need it.
- Immediately check your account statement when you receive it in the mail or online.
- Save your receipts to compare with monthly statements.
- Pay attention to what clerks do with your card while processing your transaction. Skimming (copying) your card will require them to "swipe" the magnetic strip on a second device separate from the cash register.
- If you notice unusual or suspicious charges, call your credit card company immediately to report the item.

Watch for Scams

Lower credit card rates. With this scheme, someone calls and says they're 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 e-mails 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.

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.

Web Sites to Help You With Identity Theft

Federal Trade Commission
www.ftc.gov

For Identity Theft
www.consumer.gov/idtheft

Banking Agencies

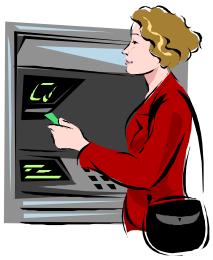
Federal Deposit Insurance Corporation
www.fdic.gov

Federal Reserve System—www.federalreserve.gov

National Credit Union Adm.—www.ncua.gov

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

Office of Thrift Supervision-www.ots.treas.gov



Ethics Darwin Awards (from the August 2002 edition of Federal Ethics Report)

One evening at a typical Washington reception, people were milling around being sociable and as invariably happens the conversation turned to work. The people started discussing the ethics questions they had encountered over the years and started comparing stories to see who had the most absurd. They discovered they had the makings for the Ethics Darwin Awards and decided to present their findings at a meeting of the Interagency Ethics Council. Below are a few of the stories.

Conflict of Interest: "Sure I can approve my own request, why not?" A Federal attorney, who was the secretary of his private sailing club, sent a letter to the Navy admiral in charge of the Navy facilities in the nearby harbor, requesting on behalf of the sailing club the use of the Navy's piers by the sailing club. Later that week, as the General Counsel for the same admiral, the attorney reviewed his own letter and recommended approval of the request. Not a bad system! Too bad the attorney violated not one, but two criminal statutes (18 U.S.C. §§205 and 208).

"My company is the best, really!" A Government computer support manager worked for a private computer repair firm during off-hours. In his official capacity, he recommended and then authorized sole source awards to that firm. When the Government found out about it and asked him what he thought he was doing, he said, "I am very familiar with the work of the firm and knew that the Government was getting the best deal from qualified people." He received a 2-week suspension without pay, and was removed from supervisory responsibilities (18 U.S.C. §208). (Those who knew the employee confirmed that he really believed he was doing the right thing.)

Outside Activities: Would cloning work? A Federal forest fighter wanted to know if he could have a part-time job with a local fire-fighting brigade. When asked if that brigade also fights forest fires, he responded in the affirmative. What did he plan to do about his regular job in that situation? His answer: take annual leave.

Use of Government Resources:

"What do you mean, I can't sell real estate at work!" A Federal employee, who had a second career as a realtor, printed her agency phone number on her realtor business card. When she answered her phone at her agency, she announced her office as "J&B Real Estate." When advised that she could not use her Government office for her commercial business, she left Federal service (5 C.F.R. §2635.704).

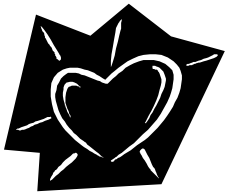
(The record is silent regarding how much of her duty day was actually spent on Government work.)

Real estate, part II. An employee at another agency set up her realty business the same way. However, when her supervisor finally took away her phone, she gave out her co-workers' phone numbers. When her personal calls came in, she took over their desks to continue her realty business. She was eventually removed from Federal service (5 C.F.R. §2635.7).

What do you mean, this isn't my property!" One entrepreneurial employee backed his panel truck up to the office door one night and stole all the computer equipment. He wasn't too hard to catch because he tried to sell everything at a yard sale the next day—with bar coding and "Property of U.S. Government" still prominently displayed (5 C.F.R. §2635.704).

Darwin Awards (cont. from page 6)

"But it makes my heart flutter!" The agency issued a policy statement prohibiting employees from viewing sexually explicit material via office computers and the Internet. About 6 weeks later, a supervisor walked into an employee's cubicle and observed that the subordinate's computer was connected to a pornographic Internet site. Also, the employee's computer log showed he had visited multiple pornographic sites for almost 2 hours. The supervisor issued a notice of proposed suspension to the subordinate for unauthorized use of government property and wasting time. The employee claimed that he viewed the sites to "cool down and relax" after an argument with this supervisor. The employee claimed discrimination on the basis of age (62) and disability (heart angina) when he was issued a 5-day suspension that was later reduced to 3 days. The Equal Employment Opportunity Commission affirmed the agency finding of no discrimination (April 5, 2001) (5 C.F.R. §2635.704 and 2635.705). *Clinton Zimmerman v Pirie, Secretary, Department of the Navy,* 101 FEOR 1223.

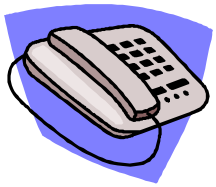


Organization

United States Nuclear Regulatory Commission

Office of the Inspector General
11545 Rockville Pike
Mail Stop T 5D28
Rockville, MD 20851

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



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