OIG Investigations Fraud Bulletin

Office of the Inspector General — January 2000 Issue
Published Quarterly

Inside This Issue

Press Releases from the IG Community

Fraud Indicators

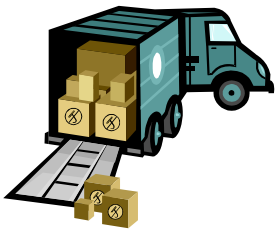
"Real" Fraud Schemes

Identity Theft

The OIG Investigations Unit has embarked on a renewed effort to detect contractor fraud. Experience has shown the overwhelming majority of government contractors are honest and conduct their activities in compliance with federal procurement rules. However, the case examples shared in this bulletin demonstrate how far some unscrupulous individuals and contractors will go to perpetrate millions of dollars of fraud each year. These examples will also show that in the majority of cases the fraud scheme was detected by dedicated government employees who displayed a questioning attitude and were willing to go the extra mile by looking behind the paper. You will also find in this edition of the Fraud Bulletin sections on "Fraud Indicators," "Fraud Schemes" and "Identity Theft."

Protection of our country's health and safety is a shared responsibility. We hope this bulletin will sensitize NRC employees to common fraud schemes and lead to detection of contractors committing fraud against NRC. Working together, we can ensure that NRC receives a dollar of goods and services for every dollar spent.

DOD Employee Indicted on False Claims



DEFENSE CRIMINAL INVESTIGATIVE SERVICE

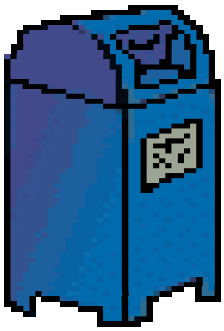
A one count indictment was returned against a DOD employee for allegedly submitting a false claim to the U.S. Government. The indictment was a result of an investigation that the employee allegedly submitted a false claim for reimbursement of moving expenses in connection with the employee's relocation from Columbus, OH, to Battle Creek, MI.

Specifically, the employee claimed that he was accompanied by his lawful wife and children on various dates from May 1998 to August 1998, during his permanent change of station relocation, which entitled him to a larger per diem or daily living expense reimbursement. The investigation disclosed that the employee's wife and children did not accompany him on many dates listed in the claim. The employee also claimed paying rent and a breach of lease penalty on an apartment in Ohio. The investigation disclosed that the employee did not make any such payments. The false claim caused losses to the United States Department of Defense in excess of $10,000. If convicted, the employee faces a maximum sentence of 5 years in prison and a $250,000 fine.

30 Years in Prison and $1M Fine Possible

DEFENSE CRIMINAL INVESTIGATIVE SERVICE

On October 13, 1999, the owner of a fire and safety company was indicted by a Federal Grand Jury in Hartford, CT on two counts of mail fraud and one count of violating the Hazardous Materials Transportation Uniform Act.



According to the indictment, the owner of AAA Fire and Safety, provided inspection services for fire protection systems. The owner and AAA falsely represented to customers that federally mandated, hydrostatic testing had been performed. The equipment was then fraudulently stamped as having met all requirements. Customers, including the DoD and the Connecticut National Guard, were then billed for the work not performed.

If convicted, the owner faces a maximum of 30 years in prison and fines of up to $1 million. The charges are the result of a ten-month investigation into activities of AAA.

DTC Settles for $400,000

DEFENSE CRIMINAL INVESTIGATIVE SERVICE

On November 15, 1999, Diverse Technologies Corporation (DTC) Clinton, MD and the United States Attorney's Office, Baltimore, MD, reached an out of court settlement in the amount of $400,000. The settlement agreement resolves allegations of systematic mischarging by DTC on two U.S. Navy contracts, which were for computer services for the Defense Finance and Accounting Service. These contracts were administered by the Defense Contract Management Command, Baltimore, MD. The contractor is an 8(a) company in the Small Business Administration program. The company admitted no wrongdoing in the settlement agreement.

DTC was awarded two U.S. Navy time and materials type contracts which called for the development of software for the Navy's financial accounting system known as Standard Accounting and Reporting System (STARS).

STARS is used in the DFAS accounting system. Each of the contracts were valued at approximately $3 million.

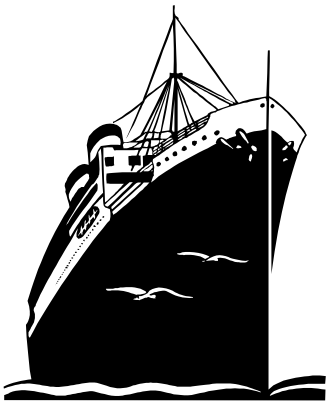
Information was developed that alleged that DTC officials were directing employees, through written memoranda, to charge their time to the Navy contracts while performing administrative duties or working on other contract proposals. Additionally, DTC was alleged to have used an overhead rate on both contracts that was fully burdened with the expenses of establishing an office in Mechanicsburg, PA, when in fact the office was never established.

Two Plead Guilty to Kickbacks

DEFENSE CRIMINAL INVESTIGATIVE SERVICE

On November 4, 1999, the president, Tidelands Testing and former partner of Gamma Tech, Industries, San Diego, CA, was sentenced in U.S. District Court, Southern District of California, San Diego, CA. He previously plead guilty to two counts of paying kickbacks to a Contract Administrator, Pacific Ship Repair and Fabrication, Inc., with regard to repairs of U. S. Naval ships.

He received a sentence of six months incarceration, ordered to make restitution of $423,689.50, and serve three years supervised release and pay a special assessment of $100.



Tidelands Testing previously entered a plea of guilty to one count of paying kickbacks. Tidelands Testing was placed on probation for a period of five years, ordered to pay restitution of $423,689.50 jointly with the president of the company and a special assessment of $600.

Gamma Tech Industries previously entered a plea of guilty to one count of paying kickbacks. Gamma Tech Industries was placed on probation for a period of five years, ordered to pay restitution of $167,231 and a special assessment of $200.

These sentences are the result of an investigation into the payments of kickbacks to Stanley by subcontractors working on the San Diego waterfront in order to receive work. Seven other individuals or entities have previously entered guilty pleas related to this investigation and are currently awaiting or have been sentenced.

Conflict of Interest

NUCLEAR REGULATORY COMMISSION

The OIG investigated an allegation regarding an NRC contractor with an organizational conflict of interest that violated NRC contract provisions. Specifically, the NRC contractor was reviewing work performed for the nuclear industry, while acting as a subcontractor for another company that was performing work for the industry. Through interviews of former company officials and reviews of subpoenaed records, the OIG confirmed that for about a year and a half, the NRC contractor had a verbal agreement with another company to internationally market strainer blockage work. The contractor's agreement with the NRC strictly prohibited the contractor's affiliation with companies doing work for the nuclear industry. Because the NRC was satisfied with the work performed under the contract, there was no financial loss to the government. Accordingly, the US Attorney's office declined prosecution of this case.

Contractor Operating Without a State License

NUCLEAR REGULATORY COMMISSION

The OIG received an anonymous complaint that an NRC contractor providing security guard services was operating without the State business license that was required under the terms of the NRC contract. In addition, the contract required the contractor's employees to carry firearms, but the employees did not possess valid State firearms permits. As a result, the OIG coordinated this investigation with the Maryland State Police, as well as another Federal agency which had a similar contract with the security firm. The NRC subsequently terminated its contract with the firm, and awarded a new contract to another security firm.

GSA & NRC Dispute Contractor Billing

NUCLEAR REGULATORY COMMISSION

The OIG initiated an investigation concerning an allegation that errors were detected in the type and number of recycled materials reported by World Recycling Company, the Government's recycling program contractor in Metropolitan Washington, DC. Through a contract with the General Services Administration (GSA), the contractor pays the Government for recyclable paper collected from Federal agencies in the Metropolitan area. However, the OIG learned that the contractor failed to report NRC pickups, thereby causing a loss to the NRC. Although the NRC successfully resolved the contract irregularities, the GSA OIG questioned whether the recycling program contractor was also under-reporting or improperly downgrading recyclable paper pickups at other government facilities. The NRC OIG and GSA OIG participated in a joint investigation and determined that

False Claim on Small Entity Status

NUCLEAR REGULATORY COMMISSION

The OIG has conducted a series of investigations involving the review of NRC materials license files to identify potential instances of fraud related to a special program under which certain licensees may claim small entity status and qualify for a reduced NRC annual license fee. In reviewing a sampling of the small entity claims made by such licensees, the OIG identified several companies that may have falsely claimed small entity status by indicating that their gross annual receipts were under the prescribed limit. In three of the investigations, the OIG determined that the licensee improperly claimed the small business entity status and improperly obtained a reduced license fee.

Trash-Hauling Firms Fined $3.3 Million in Fraud Against U.S. Navy

NAVAL CRIMINAL INVESTIGATIVE SERVICE

Two Maryland trash-hauling firms, A.W. Stevens and Sons Waste Disposal Systems, Inc., and St. Mary's Disposal Systems, Inc.,were fined a total of $3.3 million -- a $1.3 million criminal penalty and a $2 million civil fine -- following their guilty pleas in June to an array of illegal activities including false billing to the U.S. Navy of approximately $800,000.

The vice-president of the two was ordered to serve five months in jail and five months of home monitoring and pay a $30,000 fine. Three other defendants sentenced in the case were ordered to pay $20,000 fines to both St. Mary's County and Prince George's County in Maryland in connection with the case.

An investigation led by the Naval Criminal Investigative Service and the Prince George's County Department of Public Health revealed that the two firms illegally trucked garbage collected from the Navy's Patuxent River Naval Air Station, Indian Head Naval Ordnance Station and the U.S. Naval Academy in Annapolis to Virginia. The cost to the firms of final dumping in Virginia was lower than it would have been in Maryland. However, the Stevens companies billed the Navy as if the Maryland rates were being incurred, pocketing the difference. The disposal companies also operated unlicensed transfer stations for the moving of garbage from vehicle to vehicle, creating a public nuisance and polluting a tributary of Henson's Creek in Maryland.

The firms pleaded guilty to federal charges including conspiracy, making false claims, making false statements and violation of the Clean Water Act. A guilty plea also was entered to a charge of falsifying a statement to the U.S. Department of Transportation's Office of Motor Carrier and Highway Safety regarding the hours the companies' drivers spent behind the wheel.

Fire Protection Company Owner Pleads Guilty To Falsifying Cylinder-Testing Records

DEPARTMENT OF TRANSPORTATION

The owner of Taylor Fire Protection Sales and Service of Manila, Arkansas, pleaded guilty to charges stemming from his false confirmation that special tests had been performed on cylinders carrying compressed gas.

The owner, who was charged with tampering with markings the on hazardous-material containers, faces up to five years' imprisonment and a fine of up to $250,000.

An investigation by the Department of Transportation, Office of the Inspector General and the Department's Research and Special Programs Administration found that Earnest had falsely marked compressed gas cylinders handled by his firm to show they had been "hydrostatically" tested in accordance with DOT regulations, when they had not been. In a hydrostatic test, the cylinder is subjected to twice the internal gas pressure it would have to contain in everyday service. Such testing, required at least once every five years, can reveal fatigue not detectable through visual inspection. There is danger of explosion, with potential for death or serious injury, among cylinders inadequately tested for metal fatigue.

Chemist and Supervisor Pled Guilty to Falsifying Laboratory Analyses

ENVIRONMENTAL PROTECTION AGENCY

On July 21, 1999, a laboratory chemist and a laboratory supervisor, each pled guilty to making a false statement and aiding and abetting others in the commission of making a false statement. In May 1999, the chemist and supervisor of CompuChem Environmental Corporation of Cary, North Carolina, were charged with conducting improper gas chromatography/mass spectrometer analyses on samples taken from hazardous waste sites nationwide and falsely certifying that the analyses complied with all EPA contract requirements. The EPA relies on the testing data provided by laboratories participating in the Contract Laboratory Program to assess threats to public health and the environment and to determine where and when remedial action is needed. This investigation was conducted by Special Agents of the Environmental Protection Agency Office of the Inspector General.

NASA Contractor Employee Pleads Guilty

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

On November 24, 1999, a NASA contractor employee with Orbital Sciences Corp., pled guilty to one misdemeanor count of Unauthorized Use of a NASA Computer. Nance admitted he downloaded pornographic images from the Internet to NASA computers at the Goddard Flight Space Center (GSFC). Sentencing is scheduled for March 22, 2000. The investigation was conducted by Special Agents of the NASA Office of Inspector General, with assistance from the Goddard Security Office.

False Statement on Loan Application

SMALL BUSINESS ADMINISTRATION

The president of a company located in Quincy, Massachusetts, was sentenced to serve five months of incarceration, five months of home detention, and three years of supervised release.

He was also ordered to pay restitution totaling $216,838 to the Small Business Administration and two other victims. He previously pled guilty to five counts of making false statements on loan applications to a federally insured financial institution. According to the charges to which he pled guilty, he had provided false documents and made false statements to obtain two loans and a credit line, totaling $293,000. He falsely claimed that he had made an equity investment in his business, submitted false statements pertaining to the use of the loan proceeds, and submitted balance sheets containing false information about the business. The business was a wholesaler of specialty coffee and related equipment. The investigation was conducted jointly with the Federal Bureau of Investigation (FBI) and originated from a referral to OIG from SBA's Massachusetts District Office.

Misuse of Official Position to Defraud the Government

SOCIAL SECURITY ADMINISTRATION

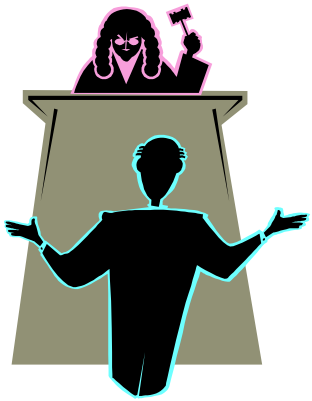
Special Agents from the Office of Investigations, Kansas City, Missouri, Suboffice conducted an investigation of two Social Security Administration (SSA) employees who misused their official positions to defraud the SSA of $174,312.30. As a Benefit Authorizer, the principal SSA employee had the ability to cause SSA benefit checks to be authorized and mailed to SSA beneficiaries. For a period of over 1 year, the employee caused unauthorized SSA checks to be made payable to herself and her relatives, friends, and acquaintances. The employee solicited a fellow Payment Center worker to further the scheme. The principal employee ensured the second employee received a sizeable sum of money by means of unauthorized SSA benefit checks if she agreed to participate in the scheme. The second employee agreed to receive the proceeds from these unauthorized checks but was afraid to have the checks made payable to her for fear of being arrested. Consequently, the second employee asked a friend to agree to be the

named payee on the fraudulently issued SSA checks in return for the payment of a sum of money. The friend agreed; so the second employee paid the friend $100 for negotiating the first check. On later checks, the second employee paid the friend approximately 10 percent of the face value of the checks (about $300 on average). In all, the second employee knowingly received and converted to her personal use $20,993.10 as proceeds from unauthorized SSA benefit checks. As a result of the Kansas City Suboffice investigation, both employees were terminated from their positions. The principal SSA employee was sentenced to serve 15 months in prison, 3 years probation, and ordered to pay restitution to SSA in the amount of $174,312.30. The second SSA employee was sentenced to five years supervised probation and ordered to pay restitution to SSA in the amount of $20,993.10.

Sentencing for Making False Statements

P O S T A L S E R V I C E

On September 23, 1999, Sharp Construction Company, Inc., (Sharp), the former comptroller for Sharp Construction, and a former project manager for Sharp, were sentenced for making false payroll reports in connection with federally funded government contracts.



Sharp Construction was sentenced to three years probation and a $25,000 fine and paid restitution. Currently suspended, Sharp also may be permanently barred from receiving future government contracts. The former comptroller was sentenced to two months in a half-way house, six months home detention, and three years probation. The project officer was sentenced to three years probation, six months home confinement, and a $2,000 fine.

On April 28, 1999**,** Sharp pled guilty to making false statements to the Department of Labor (DOL) in connection with a Department of Veterans Affairs (VA) program. Sharp aided and abetted the making and preparation of false certified payrolls and the submission of these false payrolls to the DOL. The comptroller pled guilty to conspiring to make false statements to the DOL. He prepared and submitted false certified payrolls to the DOL on a VA and US Army contract. The project officer's guilty plea is based on false testimony before the federal grand jury regarding the submission of false certified payroll to the government.

The investigation revealed that Sharp failed to pay its employees at the prevailing wage rates. Investigators from the USPS Office of Inspector General (OIG) were able to determine that during the time Sharp performed work under a USPS contract valued at approximately $2 million, he obtained approximately $14,000 from the USPS through the submission of false certified payroll reports.

Bribery by President of Cleaning Company

POSTAL SERVICE

The President of ShineBrite, Incorporated (ShineBrite), was indicted for bribing a United States Postal Service (USPS) official. He was charged in a four count indictment for making illegal cash payments to a USPS official, who was responsible for oversight and award of certain cleaning contracts for five Jersey City Post Offices. According to the indictment, he paid the Postal official to ensure that ShineBrite would continue to get the month-to-month cleaning contracts. Each count of this indictment carries a maximum of 15 years incarceration and a $250,000 fine.

"BE ALERT FOR FRAUD INDICATORS"

The Government employee, especially procurement officials and Contracting Officer Representatives, must be alert for possible instances of fraud. The best way to accomplish this is to be familiar with fraud indicators. A fraud indicator only means that a given situation is susceptible to fraudulent practices. It does not mean that fraud exists. The NRC employee's role is not to prove fraud (the intent to deceive the Government) but to refer **potential instances** of fraudulent practices to the NRC's Office of Inspector General (OIG), if he or she believes that evidence indicating fraud has been found. The OIG is trained in numerous techniques for determining whether the intent to deceive NRC exists. Remember, fraud is most likely to occur when the opportunity for undetected misconduct outweighs the chance for being caught.

FRAUD INDICATORS FOR THE QUARTER

FALSIFICATION OF DOCUMENTS

The Scenario. During a proposal review, the Government official is reviewing support for a proposed unit cost. The contractor has used actual cost as a basis for the proposal. The actual unit cost is supported by a purchase order history. The Government official performs a statistical sample of the proposed bill of material and requests the supporting documentation for the selected items. The contractor provides copies of vendor invoices. The official closely reviews the copies and notices some suspicious print type which does not match that of the rest of the invoice. The official expands the review and requests the original invoice/document. Upon receiving the originals from the contractor, the Government official notes the following:

1. The unit price on the original invoices do not match the unit prices on the copies. Apparently, some have been altered by putting additional numbers in front of the price or by moving decimals.

2. Discount terms at the bottom of the invoice have been "whitened out" so the employee would not notice an offered 20% discount.

Fraud Indicators

-- Original documentation consistently unavailable for the Government Official's review.

-- Consistently poor, illegible copies of supporting documentation.

-- Different supporting documents provided for the same items with unit prices varying widely for the same part, for no obvious reason.

General Comments. The Government employee had performed a review of the purchasing system two years earlier. During that review, no significant deficiencies were noted. The Government employee relied heavily on the results of that review and used only the purchase order history to verify unit prices. The contractor took advantage of the situation by altering selected invoices.

The Government employee should periodically reverify the integrity of the accounting and operating system he or she relies on. This can be done by doing transactional and compliance testing on a selected basis. In this case, it would involve requesting original documentation from the contractor to support the purchase order history. In other cases, the government employee may want to get third party confirmations from the actual vendors. This step might only be done on one or two transactions per proposal. The employee must be alert to changes in how a system works after he or she has reviewed and accepted it. Reliance must be based on continual review.

BEWARE: These Fraud Schemes Really Happen!

We would like to share with you some crime prevention tips concerning fraud schemes we've seen recently. We all are familiar with the new rules for traveling with our United States Government (USG) VISA cards and for making small purchases with the USG BankCards. NRC has been victimized by a type of credit card fraud which makes use of a device known as a skimmer. A skimmer is a small device about the size of a pager and can be worn on the belt. With a quick swipe of your Visa card or your USG BankCard, someone can capture all the data from the magnetic strip on your card and use that data to encode a cloned card. Since your card hasn't actually been stolen, you don't become aware of the theft of the data until after a number of charges have been made. You should avoid letting the card out of your sight if at all possible when you use your credit cards.

Don't call back 809 numbers. You may receive an email with a subject line of "ALERT" or "Unpaid account" and to call Mike Murray at Global Communications. You may get a long recording or someone who speaks broken English. They will try and keep you on the line as long as possible at $25 per minute. Another permutation is

either a phone message or a page asking you to call for info about a sick family member; to tell you someone you know has been arrested or died; or that you won a prize. These numbers are similar to 900 numbers except they aren't required to tell you of the charges for the call. The 809 area code is located in the British Virgin Islands.

Y2K: Sometime after the new year, the law enforcement community is anticipating criminals will make use of this opportunity to try and get confidential information from you. If someone posing as a representative of OCIO calls you and says they need your password and USAID to repair a Y2K problem with your account, don't give it to them! OCIO will never ask you for your password over the phone. The same holds true for calls from your bank or other financial institutions. If they call to tell you there is a Y2K problem with your account, don't give any sensitive or personal identifying information out over the phone.

Protecting Yourself from Identity Theft

Identity Theft and Credit Card Fraud are the fastest growing White Collar Crimes in the nation.

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

Detecting Identity Theft

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

- Unusual purchases on your credit cards
- Being denied a loan you qualify for
- Bank statements 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

If you suspect that someone is illegally using your identity or making charges in your name, immediately call the organization handling the account and follow up with a letter. Also, contact your local police department.

Preventing Identity Theft

- Shred all credit card, bank and other financial statements
- Always use secure WWW sites for Internet purchases
- 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 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/bank accounts and destroy old credit cards and shred unused credit card offers
- Remove your social security number from checks, Drivers ID or other ID
- Always ask for the carbon papers of credit purchases
- Do not leave outgoing credit card payments in your mailbox
- Do not carry your Social Security Card in your wallet unless needed
- **ORDER YOUR CREDIT REPORT ONCE A YEAR AND LOOK FOR ANY ANOMALIES**

If you are a victim of identity theft, you must document everything.

Identity theft involves someone utilizing your identifying information in order to acquire goods or services in your name through the use of credit or debit cards, checks, or other documents. In the worst cases, these 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 bulletin, you may be able to prevent or minimize losses due to issues of fraud and identity theft. **It is important to act quickly, effectively and assertively to minimize the damage.**

To prevent identity theft shred all papers containing financial and personal information before you throw them out. Also, 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.

What to do: Here are the initial actions victims of identity theft should take to begin the investigative and recovery process.

1. **Report the crime to your local civilian police immediately.** File a detailed police report. Give them as much documented evidence and information as possible. Keep a copy of the incident report and give it to creditors, banks, and merchants who often 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 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.

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

5. **Get copies of your credit reports,** following your initial report, monthly for at least several months to check for any new

fraudulent accounts. The credit agency 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, 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 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 only be used 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).

Know Your Rights

For more information about your credit rights, write to Public Reference, Federal Trade Commission, Washington, DC 20580 and ask for the free pamphlets:

- *Credit Billing Errors*
- *Fair Credit Billing*
- *Lost or Stolen: Credit and ATM Cards*
- *Credit and Charge Card Fraud*

Or call 1-877-FTC-HELP or surf to **www.consumer.gov/idtheft** on the Internet.

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.

The stress commonly experienced during identity theft victimization and recovery can be quit severe. Victims should consider seeking counseling assistance as an option, not only for yourself, but family members who may be equally traumatized.

Final Note: Your credit rating should not be permanently affected, and no legal action should be taken against you. 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.

IMPORTANT NUMBERS TO REPORT SSN AND IDENTITY THEFT

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
800-525-6285

Equifax Order Credit Report
800-685-1111
Experian to Report Fraud
888-397-3742
Experian Order Credit Report
800-301-7195
Trans Union to Report Fraud
800-680-7289
Trans Union Order Credit Report
800-916-8800

Fraudulent Check Use

If you've had stolen checks or bank accounts set up fraudulently in your name, call these check guarantee companies:

CheckRight	800-766-2748
Equifax	800-437-5120
TeleCheck	800-710-9898

They can flag your file so that counterfeit checks will be refused.

Here's a way YOU can help fright fraud at the NRC. Make the right choice.

Call the
HOTLINE
today.
It's your right... and duty.

1-800-233-3497

Or you may write:

HOTLINE

USNRC/OIG

Mail Stop T5D-28

Washington, DC 20555