OIG Fraud Bulletin

NRC Hotline 800-233-3497 March 2000 Issue
NUREG/BR-0272, Vol. 1, No. 1

Inside This Issue

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. This edition of the Fraud Bulletin focuses on kickback fraud and information on fraud schemes in government contracts. It also provides guidance to you in avoiding becoming the victim of some current fraud schemes, credit card fraud, phone fraud, 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.

Fraud Schemes

What is a Kickback?

This issue of the OIG Fraud Bulletin focuses on kickbacks. Payments made for the purpose of improperly obtaining or rewarding favorable treatment in relation to a government contract constitutes a kickback. Kickback schemes are arrangements between government officials and prime contractor representatives or between subcontractors and

prime contractor buyers, high level officials or even company owners.

Kickback Scheme

Generally, in these cases the government official may solicit the prime contractor to pay a percentage of all contracts awarded to the contractor. Another scenario is where the subcontractor agrees to pay a percentage of all subcontracts awarded to the subcontractor by the prime.

- ★ One kickback scheme is called a "bump" agreement. In these cases, the prime's agent tells the vendor how much he or she can raise the bid and still be low bidder.
- ★ Another system is courtesy bidding. Courtesy bidding revolves around various vendors taking turns being the low bidder. When a company is not designated the low bidder, it submits an artificially high bid to protect the designated vendor's bid.

In other instances, the contractor's agent may disclose the legitimate bids to the designated vendor so he or she can underbid the competition. The co-conspirator may also disqualify legitimate low bids on the basis of technical or financial capability and award the subcontract to the preferred vendor. The subcontractor could also pay kickbacks to a nonexistent company or one that is created solely to facilitate payments from the subcontractor to the recipient of the kickback. These payments may be for consulting services and materials which appear related to the contract, however, when compared to overall costs and other actual charges, they show up as unusual. Although such payments are similar in many ways to bribing a government official, kickbacks, until recently, had not been the focus of public attention and little had been done to address the problem. Congress strengthened the original 1946 kickback statute in 1986 (see 41 U.S.C. §§ 51-58) to make it illegal for any person to provide, attempt to provide, or offer a kickback to a government contractor or a contractor's employee for the purpose of improperly obtaining any favorable treatment under a government contract. The prohibition covers any money, commission, gratuity, or anything else of value, whether paid directly or indirectly, and applies equally to persons who solicit, accept, or attempt to generate kickbacks. The legislation further prohibits the inclusion of any kickback amounts in the contract price charged by a contractor.

Kickback Fraud Indicators:

- The same contractor repeatedly awarded competitive contracts based on bids only slightly lower in price than the next lowest competitor.

- Poor contractor internal controls over key functional areas, such as purchasing, receiving, and storing.

- Relationships which are "too close" are observed between contractor and government officials.

- Purchasing employees maintaining a standard of living obviously exceeding their income.

- Instances of buyers or other employees circumventing established contractor procedures for competition of subcontracts.

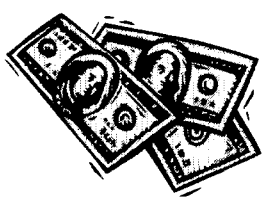
- Poor or no established procedures for competition of subcontracts.

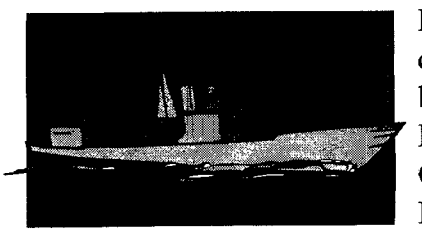
Detection of subcontractor kickbacks is difficult. Standard audit procedures normally will not uncover such schemes. The government employee must be alert to obvious weaknesses in the contractor's internal controls which make taking payoffs easy instead of difficult. Audits of the contractor's material purchasing, receiving and storing systems will point out other weaknesses or noncompliance with existing contractor policies and procedures. Physical verification of the existence of inventories or materials charged directly to a job will also show how vulnerable the contractor's system is to fraud. A management review may be the best way to evaluate the contractor's policies and procedures for awarding subcontracts. This could assure that the contractor is following the proper procedures.

Situations where fraud indicators indicating potential kickbacks are detected should be brought to the attention of the OIG for potential follow-up. Because contractors operate in a closed but close-knit community, issues/information often gets discussed. Competitors may make statements concerning rumors of wrongdoing to government employees with whom they come into contact. Such information should be brought to the attention of OIG immediately. The point NRC employees should keep in mind is that the cost of kickback payments are ultimately passed on to the contract and therefore ultimately the American taxpayers. The following are some examples of recent kickback cases.

Contracts Valued in Excess of $200 million

October 28, 1999, Joseph W. LeClair III, owner, Janco Ship Repair, Inc., Jacksonville, FL, plead guilty in U.S. District Court, Jacksonville, FL, to a one count information filed in the Middle District of Florida, Jacksonville, FL, charging him with paying kickbacks and to a one count information, filed in the Eastern District of Virginia, charging him with one count of bribery. Janco Ship Repair, Inc., also plead guilty to a one count information, filed in the Middle District of Florida, charging the company with paying kickbacks. These guilty pleas are the result of a 3 ½ year undercover investigation into fraud and corruption within the Maritime Industry conducted by the Defense Criminal Investigative Service, Naval Criminal Investigative Service, and the Federal Bureau of Investigation. Janco Ship Repair, Inc. was a subcontractor to Bay Ship Management, Inc., Englewood, NJ, and performed repairs aboard the United States Navy's Military Sealift Command (MSC) ships. Bay Ship Management, Inc. had multiple contracts, valued in excess of $200 million with MSC, and provided operational and





technical support to operate and maintain eight MSC ships. LeClair and Janco Ship Repair, Inc. plead guilty to paying kickbacks and bribes to Cary Gordon Byron, senior port engineer, and Robert Collins, port engineer, Bay Ship Management, Inc., in return for favorable treatment related to the subcontracts.

Patient Referrals Resulted in 78k in Kickbacks

The former director of internal medicine, Bridgeport Community Health Center, Bridgeport, CT, was sentenced in U.S. District Court, Bridgeport, CT to 4 months imprisonment, 4 months home confinement, 4 years probation, $200 special assessment fee and a $10,000 fine. He plead guilty to one count of soliciting and receiving kickbacks in connection with the disbursement of Medicaid funds, and one count of willful subscription of a false Federal Income Tax Return for the calendar year 1997. According to the information, the director received approximately $78,130 in kickbacks in connection with referrals of patients to R&R Surgical Supplies, a durable medical equipment company located near the Bridgeport Community Health Center. The investigation is the result of a 3-year undercover operation, code-named "Operation: Overdraw." Overdraw established an undercover medical "business" that dealt with dozens of health care related companies in Connecticut, New York and New Jersey suspected of engaging in fraudulent activities associated with Medicare, Medicaid, private insurance companies and TRICARE, formerly known as the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS).

NASA Subcontracting Official and Corporation Sentenced

On November 19, 1999, John W. Knight, and his corporation, Aall American Fasteners, Inc., a former NASA subcontractor located in Vincentown, New Jersey, were sentenced in U.S. District Court, Orlando, Florida, for paying kickbacks. Knight was sentenced to 3 years probation, was ordered to pay a $50 special assessment, $7,909 in restitution and fined $1,000. Aall American was ordered to pay a $200 special assessment.

Knight and Aall American both plead guilty on September 2, 1999, to one count of paying kickbacks in violation of Title 41 USC Section 53. Knight admitted he paid in excess of $7,900 to Michael F. McCusker, a procurement official at Lockheed Martin Services, a NASA prime contractor located in Cape Canaveral, Florida, in return for Aall American being awarded over $79,000 worth of NASA subcontract business from Lockheed Martin Services. Aall American provided fasteners to Lockheed Martin Services. These fasteners

were used in items related to NASA science payloads and payload support structures. In a related investigation, Michael F. McCusker plead guilty and was sentenced on February 19, 1999 for receiving kickbacks.

$900,000 Restitution to be Paid

On November 4, 1999, Michael Gallegos, President, Tidelands Testing and former partner Gamma Tech Industries, San Diego, CA, was sentenced in U.S. District Court, Southern District of California, San Diego, CA. Gallegos previously plead guilty to two counts of paying kickbacks to Loyd Dean Stanley, Contract Administrator, Pacific Ship Repair and Fabrication, Inc.,(PACSHIP) with regard to repairs of U.S. Naval Ships.

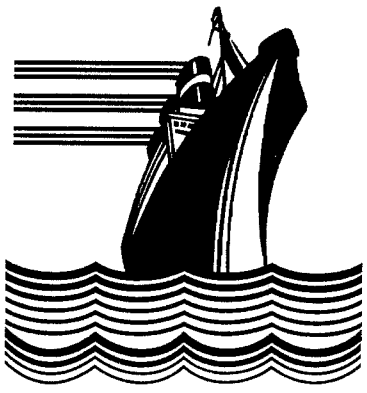
Gallegos received a sentence of 6 months incarceration, ordered to make restitution of $423,689.50 and serve 3 years supervised release and pay a special assessment of $100.

Stanley, a former Contract Administrator of Pacific Ship Repair and Fabrication, Inc. (PACSHIP), San Diego, CA, was sentenced by U.S. District Judge Rudy Brewster, Southern District of California, San Diego, CA. Stanley received a sentence of 15 months confinement, 3 years probation, restitution of $913,820.50 (to be paid jointly with the other Defendants) and ordered to pay $200 in special assessments.

Stanley previously entered a guilty plea to two counts of receiving kickbacks while employed by PACSHIP and he was responsible for the awarding of U. S. Government subcontracts to companies working on U. S Navy ships.

Falacino Vega, a former employee of Tidewater, pled guilty to two counts of failure to file income tax returns for the kickback payments he received. Vega was responsible for cashing checks made out to him from Tidelands Testing and returning the money to Gallegos, the company president, who would then pay Stanley, the contract administrator, a kickback for contracts awarded. Vega was sentenced to one year supervised release and required to pay a special assessment of $50.

Tidelands Testing previously entered a plea of guilty to one count of paying kickbacks. Tidelands Testing was placed on probation for a period of 5 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 5 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. Six other individuals or entities have previously entered guilty pleas related to this investigation and are currently awaiting or have been sentenced.

IDENTITY THEFT

1. What is Identity Theft?

Identity Theft and Credit Card Fraud are the Fastest Growing White Collar Crimes in the Nation.

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.

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.

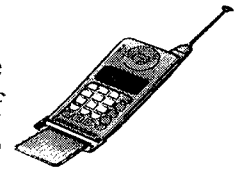
2. Detecting Identity Theft

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 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

- ♦ Shred all credit cards, bank, other financial statements and personal information
- ♦ 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 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 and promptly review all bank, credit cards 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**

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

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.**

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 process.

1. **Report the crime to your local 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.

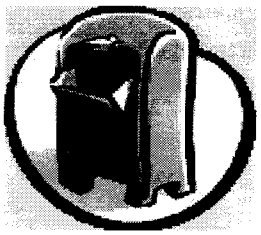
8. Give the bank, credit card and utility companies a **NEW secret password and PIN numbers** for new accounts. Do not use old PINs, passwords or your mother's maiden name.

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).

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. 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.

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.

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

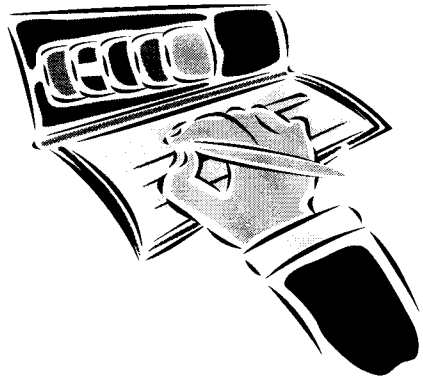
If you've had checks stolen or bank accounts set up fraudulently in your name, call these check guarantee companies:

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

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

FTC-1-877-FTC-HELP

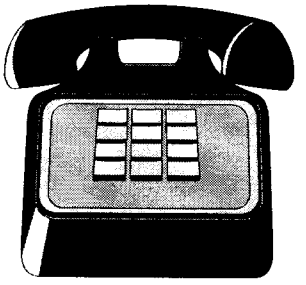
WWW.consumer.gov/idtheft



This is the first in a series of bulletins intended to assist you in supporting the OIG in making NRC programs more efficient and effective. We welcome comments and suggestions for future editions, as well as areas where OIG can support you, the NRC employee, in our mutual mission of ensuring the health and safety of our nation.

Here is a way YOU can help fight fraud at the NRC. Make the right choice.

Call the Hotline today. It is your right and duty....



1-800-233-3497

Or you may write:

USNRC/OIG
Mail Stop T5D-28
Washington, DC 20555