

2008 Reported Fraud & Scams

"Once You Have Been Scammed You Are A 'Preferred Customer'" (Oct. 6, 2008)

Senior Resources AAA reported to us that a senior in Brooklyn, CT received a phone call from James Brown (Federal Bureau of Consumer Affairs, Washington, DC) phone number 202-629-9160. He was instructed to choose one of 3 methods to transfer \$1966.72 to a Jeffrey Dunnemann in Veijo, California 92691 in return for a \$400,000+ check. He indicated that he would pay by Western Union (where "Jeffrey" would collect the money. He was also advised that once the transfer was made a Jennifer Goldstein (Office of The State Farm (!)) would be sent by car to his house between 3:00 and 4:00 to deliver the check, drawn on the Chase Manhattan Bank. Before he would send the money he spoke to John Cooper (212-660-0287) from the IRS in NY. He was told that when Jeffrey got the money he would activate a Proper Registration Policy. Our senior received an additional call on Tuesday, at which time he asked that any paperwork be faxed to his daughter and he gave his daughters phone number for them to contact her. No contact was attempted by the individuals, but when the daughter tried to make contact from her home phone she only received a recording. She went to her father's home and used his phone and was able to talk with the parties. On Thursday our senior received another call, this time from a woman stating that she was from Georgia and continuing this same scam. He hung up on her without getting a phone number. Two other names are in the mix -- perhaps a Mack Conrad and Jessica Goshen. Of course, our senior's major concern is that the scammers have his address and will continue to call him. The Reverse Directory indicates that the numbers are active unlisted numbers in Manhattan and Washington, D.C. Here is the kicker: Our senior was previously the victim of the \$295 / \$395 scam earlier this year when he gave permission for the funds to be withdrawn from his account.

"\$279 Scam is Back!" (Septebmer 10th, 2008)

It is my displeasure to report to you the \$279 scam is back in the area. We've seen this type of scam in the area before, and it appears to be back in town. A woman in Vernon called after receiving a phone call from a "Kevin Johnson with American Medical Benefits." She reported that when she got off the phone with him "She knew something wasn't right." This "Kevin" provided the elderly woman with a bogus phone number (646)164-6411 and an ID# 101 to make the call sound legit. He told the woman he was calling to provide her

with the new insurance card she "had to have in order to keep her Medicare benefits" and frightened her by saying if she didn't take the card "she would end up poor because she would have to pay for all of her medical expenses out of her own pocket!" This new card he was calling for "only cost a one time payment of \$279 and she would be all set for life." The Scam man then proceeded to gather the woman's routing number, bank account number, check number, and date of birth. As soon as she hung up the phone, she knew something was wrong and reported it to the CHOICES SMP program at the North Central Area Agency on Aging. The bank was immediately contacted to halt any further transactions from the bank as well.

"Medicare Card Scam in the Northwest" (September 4th, 2008)

The following medicare card scam started in Washington State, then Oregon, and Idaho and could be headed your way next. "People are calling from a company called National Medical Office in Washington DC," say Idaho Dept. of Insurance coordinator Krista Robinson. This "National Medical Office in Washington DC" doesn't exist. These Medicare imposters are calling seniors saying they need to get account information to send them their medicare card. "They say they cannot ask for your social security # but try to get your personal info," explained Robinson. They ask where you bank and then look up your routing number. Once they have your routing number then they try to get the rest of your bank account information says Robinson. And if you don't give it to them the caller gets very irrate and proceeds to threaten the party they are calling. Medicare stresses that they do not call their beneficiaries and if you do receive a phone call from someone claiming to be from Medicare here's what you should do: Ask if you can have their phone number and say that you will call them back. also ask to speak to their supervisor.

"Telephone Scam - Just Stay on the Line - in South Windsor" (August 20th, 2008)

From the NCAAA...Right in our own backyard, an elderly woman in South Windsor reported this case yesterday. Someone called her two times yesterday and a recording said to stay on the line and then the phone hung up. The same caller called back again today and told her they had her bank account number and how they needed her to provide some additional information. She immediately hung up the phone and called her bank and the South Windsor Police Department. The phone number on her caller ID was (860)327-0114 and when called - identifies itself as "INTL." A reverse look up of the number showed the call came from a landline in Manchester, but no name or

company name was published. Since the report was made, now only a fast busy signal can be heard when dialing the number.

This senior was on her toes and did all the right things, including calling the local police department. It is scammers like this who instill fear of identify theft and fraud into the person who answers the phone and plays on their emotions. If anyone calls and says they are from your bank or have your bank account - Don't Give Them Your Information! Instead, say you'll give them a call right back. Hang up. Call your bank, your police department and your local Senior Medicare Patrol.

"Connecticut Senior Information Update! Green Postcard" (August 4th, 2008)

From the NCAAA....An Elderly couple in the Bristol Area recently received a green postcard in the mail marked "Connecticut Senior Information Update!" When they received it they brought it to their daughter-in-law for review as it seemed too good to be true, and she agreed! Basically, the post card announces the "Senior Final Expense Program" will pay 100% of all funeral expenses not paid by government funds (up to \$25,000). The notice also says "this is a Free Service to you!" In really small print you'll read "not affiliated with or endorsed by the Social Security Administration." After surfing the internet trying to find anything that might legitimize this "program" we still haven't been able to find anything. There are however, plenty of listings from people and agencies questioning the same thing. It's almost guaranteed that anyone's best bet will be to go to someone you know and trust when looking at programs and entitlements....Scammers pounce on the opportunity to lure individuals out and take them for what they're worth.

"Capital Financial Inc. - Over the Border Canadian Scam" (July 7th, 2008)

A senior in Killingly, CT reported receiving a letter from Capital Financial, Inc., a few days ago indicating that he was one of a category of winners in the "Mega Millions Draw" held in April, 2007. Enclosed was a very real looking check for \$4,200 referred to as a Tax Clearance Fee that had been deducted from the winnings. He was advised to contact claims agent Charles Brown for information about processing his winnings at 1-604-778-865-9713. This senior was tempted to go to his bank and deposit the check, drawn off the account of NUCENTCOM Inc. a telecommunications company out of Dallas. Others receiving the same or similar letters were advised by the claims agent to deposit the check in their checking account and

then forward a money gram or a check for \$3,200 to a named "tax agent" who would forward them their winnings. Oh, by the way, the claims agent told them not to show the letter to the bank. The check WILL BOUNCE - and the consumer will be out at least the \$3,200 sent. The RIPOFF Report (www.ripoffreport.com) includes a vast number of consumer reports over the past several months relating similar fact situations - only the names are different. Unfortunately, several of the consumers fell prey to this all-too-common "over the border" scam. We googled Capital Financial Inc." and were directed to the Ripoff Report. Again...didn't enter the sweepstakes? Required to pay money to receive proceeds? Advised to be secretive? If it is too good to be true, it is...and it also is a scam.

"Guaranteed \$25,000 Grant from the U.S. Government" (July 2nd, 2008)

One of our Senior Center Directors in southern CT contacted us about a green postcard that numerous folks in her area have been receiving. The postcard states "Urgent: Read Immediately - Our Office has been trying to contact you. You are Guaranteed a \$25,000 Grant from the U.S. Government." There is no return address - just a tollfree phone number: 1-877-303-3788 and an "Official Form Number." When we called the number, a prerecorded message said (6 times) that we could receive "\$25,000 or more in free government grant money guaranteed" from their grant guide for a small payment of \$59.00 "risk free." Just dial 1..... Following a quick Google search of the phone number, we have determined that the "mailer" is ASI inc. 4149 Pennsylvania Ave. Suite 301 Kansas City, MO 64111 Office: 913-731-2478 - and that ASI is mailing 80,000 postcards daily all over the country. What is most disturbing is that the message indicates that the name, address, and number will be put into their system to facilitate the mailing - just dial 1. Who knows what will be done with that information later. If it sounds too good to be true, then it is!

"Phone Scam about New Medicare Card" (June 24th, 2008)

The following alert was forwarded from the Agency on Aging of South Central CT about a Phone Scam in the Morris Cove section of New Haven:

A Medicare beneficiary called to confirm that Medicare was going to be issuing new Medicare numbers as the caller she just hung up with had told her. She was told that there were no plans for Medicare to reissue new numbers. She retoted "I've just been scammed" and became very upset. The person who called her confirmed that her bank was Wachovia. She was instructed to contact her local Wachovia

bank branch to report the incident as well as the New Haven Police Department. The sad thing is that she called the AASCC to inquire about the potential new number after the fact.

Although this is not a new scam, events of the past week have certainly made it more lucrative for scammers. Last week information about a federal bill being introduced to fund healthcare fraud work included a provision to eliminate SSN's as the identifier for Medicare beneficiaries. Also, an article by Robert Pear "Agency Sees Theft Risk for ID Card in Medicare" was published on June 22nd in newspapers across the country, indicating that the Social Security Administration is calling for the immediate removal of SSNs from Medicare cards. As one of our CHOICES staff members commented: "It just shows these scammers are on their toes and as quickly as a story hits, they are using it to their advantage."

"Business Proposals from Attorneys in Spain?" (June 18th, 2008)

A resident in Orange, CT received a letter stating "business proposal" from an attorney in Barcelona, Spain. The attorney states his client passed away and now the bank is holding a large amount of money. He asks for her consent to present her to the bank as the next of kin since they have the same last name. This way the proceeds can be paid to her account. All he wants for his services is 10% and she can have the other 90%.

This just screams SCAM! You know what will happen, after she responds the attorney will ask for her bank account number to wire over to her the money and bingo - her account will be cleaned out. If he can't get her account # then he will state he understands, and then agrees to have the money sent to him first. He will then suggest sending her a check and he will want her to return to him the 10% or \$1,250,000. Then of course, his check will come back in 2 or 3 months as bogus, leaving her out in the cold.

Just to confirm, a check of Attorneys in Barcelona, Spain was made (lots of them). However, no attorneys by his name came up!

"Still Stuck at the Canadian Border - Send Me Your Money" (June 13th, 2008)

The New Haven Register reported the following story. North Haven Police are warning residents not to fall for an apparent scam connected to a female calling elderly residents for money. Captain James Merrithew said police have investigated 3 recent attempted scams,

with one resident losing \$1,500. "During the past few days a female has called and identified herself as the granddaughter of the resident. The phone connection is poor and the woman pleads for money to be sent to any branch of a chain of businesses similar to Western Union," Merrithew said. The woman said she was having trouble with Canadian authorities at the border. The scam victims were provided with a telephone number that starts with the Montreal area code, 514. The detective bureau has a number that may be traceable and has been in touch with the Quebec Provincial Police, Merrithew said. Residents who are called should obtain the caller's phone number, should not provide personal information and then should contact police. Merrithew can be reached at (203)239-5321. ext 740.

A similar scam was first reported in Dec. of 2007 also telling scam victims that a person was stuck at the Canadian border in need of money to get back home to the US.

"Economic Stimulus Payment Scams" (June 4th, 2008)

As you know, starting in May 2008, the US Treasury began sending economic stimulus payments to more than 130 million US households. To receive a payment, taxpayers must have a valid Social Security number, \$3,000 of income and file a 2007 federal tax return. The Internal Revenue Service (IRS) is responsible for processing and disbursing payment. Eligible people will receive up to \$600 (\$1,200 for married couples), and parents will receive an additional \$300 for each eligible child younger than 17. Millions of retirees, disabled veterans and low-wage workers who usually are exempt from filing a tax return must do so this year in order to receive a stimulus payment. There are still many older adults and persons with disabilities who have not filed returns to obtain the stimulus payments. Returns must be filed no later than Oct. 15th, 2008.

Please be aware that identity thieves are currently pushing telephone and e-mail scams involving the stimulus payments. The IRS has confirmed and documented a number of the scams: the rebate phone call, refund e-mail, audit e-mail, changes to the Tax Law e-mail, and the paper check phone call. Consumers are advised to initiate direct contact by typing IRS.gov rather than clicking on a link in an e-mail or opening an attachment. A special mailbox has been established by the IRS, phishing@irs.gov, to receive questionable e-mails and telephone calls.

"American Home Services / Pharma Bay Scam" (June 4th, 2008)

The Center for Medicare Advocacy reported a woman from Naugatuck received a call on June 3rd from a woman who claimed to be from American Home Services/Pharma Bay. The woman said that all Medicare beneficiaries were required by law to make a one-time \$374 payment to PharmaBay in order to have prescription drug coverage. (This is not true!) The woman said she was calling to let the client know they were going to debit her bank account for \$374. The woman claimed to know the client's bank and account number and said that the client had already "signed up" for this "program" a year ago. The client denied ever signing up for any such thing. She refused permission for the deduction and was then told "in that case, you will be ineligible for prescription drug coverage for the rest of your life." The woman received a confirmation number and a customer service number 1-877-393-0404. That number identified the company as Household Health Services. Further research reveals that this number has been associated with Solomon Health Group in the past with a similar scam (using the phone number 425-963-7342) in 2007 which announced that the consumer had won a federal grant and had to pay the processing fee of \$359. The client contacted Consumer Protection, The CT Dept. of Insurance and her bank.

"Scammers Seeking Bank Account Info for Health Coverage Policy & an Initial Payment of \$189" (May 22nd, 2008)

The AASCC received a call from a Milford woman reporting a man called her from an insurance company located in Washington. Supposedly the man had her personal information, including part of her bank account #, but needed her to provide him with the remaining digits. She said he needed the information so he could deduct the initial \$189.00 so he could send her information about the insurance policy he was offering: medical, doctors, hospitalization, prescription drug coverage. He told her the Center for Medicare and Medicaid Services in Baltimore gave him her information. Immediately she knew that this was a scam once he made this state. The Centers for Medicare and Medicaid Services does not give out personal information to insurance companies seeking new members. The woman next contact her bank to alert them of any suspicious activity and also contacted the Milford Police Department.

"Scam E-mails Seek Donations to Help Chinese Earthquake Victims (May 22nd, 2008)

The FBI is asking people to be aware of e-mails claiming to be raising money to help the victims of the recent earthquake in China. Tragic incidents such as 9/11, Hurricanes Katrina and Rita, the Minnesota Bridge collapse, and the Virginia Tech shootings have all prompted

individuals with criminal intent to solicit contributions for a charitable organization and/or a good cause. Some of the Chinese earthquake scam messages claim to be offering free vacation trips to the largest donors and even use fake logos of legitimate online pay services to fool people. Everyone should consider the following:

- Do not respond to unsolicited (SPAM) e-mail.
- Be skeptical of individuals representing themselves as officials soliciting via e-mail for donations.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders.
- To ensure contributions are received and used for intended purposes, make contributions directly to recognized organizations rather than relying on others to make the donation on your behalf.
- Validate the legitimacy of the organization by directly accessing the recognized charity or aid organization's website rather than following an alleged link to the site.
- Attempt to verify the legitimacy of the non-profit status of the organization by using various Internet-based resources, which also may assist in confirming the actual existence of the organization.
- Do not provide personal or financial information to anyone who solicits contributions: providing such information may compromise your identity and open you to identity theft.

"Scammers and criminals come forward after many of these tragic events and you should be wary of solicited requests for money. People should feel free to make donations, just make sure you know who are are dealing with and where the donations are going. This was you can make sure your money really makes a difference and helps out a needy person, not a greedy criminal," said Special Agent Richard Kolko, Washington, DC.

"American Health Benefits" (May 13th, 2008)

A New Haven resident said she received 3 calls from representatives from "American Health Benefits." Her caller ID indicated the call was coming from phone number 800-223-9113 and the last person she spoke with identified himself as Nicholas J. Thomas, supervisor, badge 1326, and they told her they wanted to discuss health benefits with her. The first caller told the woman that his company was working with people in the New Haven area and she had been selected to win

\$100 in free gas. He knew her address and phone but needed to verify her date of birth and provide him with her bank account information including branch number. She refused and the 3rd caller (Nicholas) became very aggressive with her and asked her why she was giving him and his staff such a hard time. At that point she hung up and called CHOICES. She also contacted the New Haven Police Dept. to file a report and then to notify her bank just in case there was any strange activity with her account even though she did not release any information.

"You Won 2.5 Million - Just Give Me Your Credit Card Number" (March 25th, 2008)

A CT Senior called her Municipal Agent on 3/20/2008 indicating that she had received a call from a gentleman called Randall Brakemeyer at 1-876-453-5534 who was very difficult to understand as a result of his broken English. He told her that she won \$2.5 million dollars and asked her for her credit card number. She told him that she did not have a credit card. The man told her to meet him that same day at a Western Union Site in Bristol at 4pm so that he could give her the \$2,500 (note the difference in dollar amount). The Municipal Agent contacted the Bristol Police Department immediately so maybe they met the man at Western Union instead! If you really won some kind of lottery prize, no one would need your credit card number to give you the winnings.

"Can You Give Me \$18.88 to Repair My Radiator Hose?" (March 20th, 2008)

We have received several reports from the South Central region of CT of a similar scam occurring in parking lots of large stores. A woman (victim of this scam) was in her car in the Branford Kohl's parking lot when she was approached by a lady knocking on her car window. The lady told the victim that she was having radiator hose car problems and she had left her purse in her daughter's car. She then asked the victim if she could give her \$18.88 to help with the repair of the radiator hose? The victim said the lady was very flustered and believable. In the midst of her request for money from the victim, the scam artist complimented the victim on her jacket. Later that week the victim was in her car in the Walgreen's parking lot in Branford and the SAME scam artist approached her with the very same story (including the same jacket compliment). This time the victim took careful note of the scam artist's physical description: brownish/reddish hair with heavy caked-on makeup, she wore a dark pea coat and appeared to have a Dark Blue Jeep driven by a male

accomplice. The victim contacted the Branford Police Department, but the scam artist and her driver left before the police arrived.

Since this story was first reported we have heard from other people who also claim to have been victims of this scam artist in a gas station in Hamden near Putnam Plaza, Home Depot in Hamden, CVS in Hamden and the Stop & Shop Plaza in East Haven. In some instances she told her victims that her daughter had her wallet and she was trying to pick her daughter up, and she has also told her victims that she is a nurse at the VA. Remember to contact your local police department if you are a potential victim of this scam artist.

"Solicitations of Personal & Health Information" (March 13th, 2008)

The following alert was received by Legal Services Developer colleagues in Alabama, North Carolina and South Carolina. Although the organization appears to be legit, the practice involved in the following description is complex and extremely risky for older adults. If you have any knowledge of solicitations of this nature happening in CT, please contact us.

The South Carolina Lieutenant Governor's Office recently circulated information to senior care professionals concerning solicitors who were offering older adults \$1,000 in cash or merchandise in exchange for their medical information. The solicitors and the company they worked for were "asking seniors to provide extensive personal information, including social security number, Medicare number, financial details, and all health information. The senior also completes an IRREVOCABLE Durable Limited Power of Attorney that gives the company the right to lifelong access to the individual's medical records and he signs a form authorizing and directing his heirs and assigns to provide a copy of the Death Certificate. In exchange for completing this 'survey' and participating in the program, the senior is given \$1,000 immediately and receives \$250 per year for the rest of their life. The packet is extensive and confusing, and improper use or disclosure of the information will put seniors at risk for financial exploitation and identity theft." The presentation are being made by members of the "STOLI" (Stranger Oriented Life Insurance) industry. The company may use the senior's personal information to purchase an insurance policy insuring his or her life, or it may sell the senior's personal information to speculators who will do so. See the following news article for a lengthier description of the business practice and California legislative hearings concerning it:

<http://www.kcra.com/news/15189803/detail.html>

"Unauthorized Use of NCOA's BenefitsCheckUp" (March 7th, 2008)

An advertising flyer circulating in the Philadelphia metro area falsely implies an affiliation between the National Council on Aging (NCOA) and an organization called "The Benefits Checkup Group." The flyer advertises new changes in Medicare benefits and provides a phone number to call. "The Benefits Check Up Group" is not related in any way to either NCOA or to BenefitsCheckUp a trademarked web-based service maintained by NCOA. the use of NCOA and the BenefitsCheckUp name is unauthorized. The phone number on the flyer appears to have been disconnected. Our fear is that whoever developed this flyer will try again to use this implied endorsement to reach vulnerable elders in the city. Beyond unauthorized use of the BenefitsCheckUp name and services, it also breaks many marketing rules set forth by Centers for Medicare and Medicaid Services. The matter has been referred to the Pennsylvania Department of Insurance and Attorney General's office for further investigation. If you have any insights concerning who may be behind this flyer or the name "The Benefits Check Up Group" please feel free to e-mail Stuart Spector, Senior Vice President - National Council on Aging at Stuart.Spector@ncoa.org. NCOA's BenefitsCheckUp is an online screening service designed to help people over age 55 find and enroll in benefits programs. The service can be accessed at www.BenefitsCheckUp.org.

"Imposter In Our Midst!" (March 6th, 2008)

The North Central CT Regional CHOICES Coordinator received the following report from a senior housing complex in Wethersfield. An elderly woman residing in the housing complex answered a phone call from a gentleman at 7 pm on a Friday night who claimed to be with the State of CT and was "calling to confirm her appointment with the Municipal Agent for the Town" (he used the Municipal Agent's First and Last Name) for the coming Monday at 9am. This wise woman was concerned about the call given the time of night and content being discussed by the caller so she hung-up. The Municipal Agent is a CHOICES counselor and was very upset to learn someone was using her name and relationship with seniors in that town to possibly do harm. If you have not scheduled an appointment with a Town or State employee, or a CHOICES counselor do not give these people any information over the phone or invite them into your home.

"IRS Telephone Scam Alert" (Feb. 25th, 2008)

The following report was brought to our attention through the Aging Network in the South Central Region of CT.

"A female resident in Orange received a call from someone claiming to be from the IRS. He asked to speak to the owner of the phone (it is listed in her husband's name). She had a funny feeling so she said she was the owner. The caller claimed to be from the IRS and her phone # was chosen to receive \$5,000 directly deposited into her account. At this point she asked the caller "what do you want my account# for? You are talking to the wrong senior." The caller became irate, swearing at her in a foreign language, and then in English. At that point she hung up and reported it to the Elderly Services Worker in the town. The phone # that showed up on her caller ID was (203)285-3059. when the worker checked the phone # on the internet he found a log stating someone else received a call from that number but left no message on their answering machine. when they called it back it was out of service. The worker then called the phone # and he also received an out of service message."

"SPAM Alert - Storm Worm Virus" (Feb. 11th, 2008)

With the Valentine's Day holiday approaching, be on the lookout for spam e-mails spreading the Storm Worm malicious software (malware). The e-mail directs the recipient to click on a link to retrieve the electronic greeting card (e-card). Once the user clicks on the link, malware is downloaded to the Internet-connected device and causes it to become infected and part of the Storm Worm botnet. A botnet is a network of compromised machines under the control of a single user. Botnets are typically set up to facilitate criminal activity such as spam e-mail, identity theft, denial of service attacks, and spreading malware to other machines on the Internet.

The Storm worm virus has capitalized on various holidays in the last year by sending millions of e-mails advertising an e-card link within the text of the spam e-mail. Valentine's Day has been identified as the next target. Be wary of any e-mail received from an unknown sender. Do not open any unsolicited e-mail and do not click on any links provided. If you have received this, or a similar e-mail, you can file a complaint at www.ic3.gov.

"No Cost Medical Card for the Elderly and Disabled (Feb. 4, 2008)

Is there really a no cost medical card that every disabled, elderly, or low-income person can get through the mail to get their medications with no co-pays? Too good to be true? We have received the following information from our CHOICES Regional Coordinator in the South Central region.

An elderly East Haven woman and her disabled daughter received 4 phone calls within a two day period. When the daughter started to ask the caller questions, the caller immediately hung up and almost instantly, another caller called back. The caller said that every disabled, elderly, or low-income person was going to receive a medical card at no cost in the mail. The card would allow people to get their medications with no co-pays. The caller asked to speak to the older woman [mother]. The daughter happened to pick up the phone and the caller said "oh, you must be [daughter's name]...we need your mother [mother's name]. Somehow, they knew their names.

The caller (who had a very heavy accent) said her name was Tharma Bay (spelling uncertain) and the call back number was 1-866-380-1481. She asked the ladies for their direct deposit account information. With this, the mother and daughter hung up and called CHOICES. The CHOICES Counselor called the phone number and, initially the message said that if you set up your account within the last 48 hours, to call back to get an update on the status of your account. The CHOICES Counselor held on until a human picked up the phone. The lady who answered the line said that she was on a customer service line and basically was just a third party. She asked the Counselor for her phone number so she could check the status of her application and also asked if she already provided her bank account information. She told the Counselor that the name of the company was "Harmer Bay" and they "take money from your account and the consumer saves 50% on prescription drugs."

The CHOICES Counselor did some further research and found that the South Dakota Senior Medicare Patrol (SMP) reported back in 12/06 a similar situation (same phone number) except in that case, the caller identified themselves as being from the Social Security Administration. However in that case, \$389 had been deducted from a person's bank account. The bank reversed the charges and the case was handed over to the SD Attorney General's Office"

"How Are You and Your Family/ Serviceman E-mail Scam" (Feb. 1, 2008)

We received the following scam from a TRIAD member who has been working with People's United Bank. This is a sad new twist on how to gain bank account information. The poor grammar and punctuation (fraud awareness tip!) are listed just as they appear. Please see the below e-mail:

"Hello Friend,

How are you and your family? Hope all is well. My name is (SFC 1st Class) Williams George; I am an American Soldier, serving in the military with the Army's 3rd Infantry Division; With a very desperate need for assistance, I have summed up courage to contact you. I found your contact particulars in an address journal and I am seeking your kind assistance for move the sum of (\$8 million U.S Dollars) eight million U.S. dollars to you in United States, as far as I can be assured that my share will be safe in your care until I complete my services here.

Source of money: some money in various currencies were discovered in barrels at a farmhouse near one of Saddam's old palaces in Tikrit-Iraq during a rescue operation, and it was agreed by Staff Sgt Kenneth Buff and I that some part of this money be shared among both of us before informing anybody about it since both of us saw the money first. This was quite an illegal thing to do, but I tell you what; Sir, no compensation can make up for the risk we have taken with our lives in this place of which my brother in-law was killed by a road side bomb last time. For further information on this, you will find the story of this money on the web address below (address removed for consumer safety).

However, the above figure was given to me as my share, and to conceal this kind of money became a problem for me, so with the help of a British contact working here and his office enjoy some immunity, I was able to get the package out to a safe location entirely out of trouble spot. He does not know the real contents of the package, and believes that it belongs to a British/American medical doctor who died in a raid here in Iraq, and before giving up, trusted me to hand over the package to his family in United States. I have now found a very secured way of getting the package out of Iraq to your country for you to pick up, and I will discuss this with you when I am sure that you are willing to assist me, and I believe that my money will be well secured in your hand because you have fear of God.

I want you to tell me how much you will take from this money for the assistance you will give to me. One passionate appeal I will make to you is not to discuss this matter with anybody, should you have reasons to reject this offer, please and please destroy this message as any leakage of this information will be too bad for us soldier's here in Iraq. I do not know how long we will remain here and I have been shot, wounded and survived two suicide bomb attacks by the special

grace of God, this and other reasons I will mention later has prompted me to reach out for help, therefore I honestly want this matter to be resolved immediately, please contact me as soon as possible. God bless you and your family.

SFC. Williams George
3rd Infantry Division"

"IRS TAX Refund Scam - Again but With a Lager Refund - Still A Scam!" (Jan. 26th, 2008)

The following e-mail is circulating again & is supposedly from the IRS. We initially reported this scam back in Oct. of 2007 - but as you can see, the refund amount indicated in the e-mail has increased. While tax season is upon us, this may seem tempting for some - but this is another scam. The text of the e-mail is below:

"After the last annual calculations of your fiscal activity we have determined that you are eligible to received a tax refund of \$480.23. Please submit the tax refund and allow us 3-9 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. To access the form for your tax refund please click here....."