*** FRAUD ALERT ***

Threats and Demands from Callers or E-mailers Impersonating Treasury Officials

The U.S. Department of the Treasury, Office of Inspector General (TOIG) issues this fraud alert to warn citizens of a recent and widespread scam. Criminals have been contacting U.S. citizens by electronic mail and by telephone and falsely claiming to be Treasury officials. The criminals then inform the victims of a "tax deficiency" or other made-up offense, and threaten imminent arrest, foreclosure, deportation, or other dire consequence unless the victims make immediate payment using pre-paid debit cards.

The electronic mail version of the scam is often accompanied by colorful and elaborate but fraudulent "official government documents," including a copy of the sender's "credential" or other identification. The documents are all fake but some are good enough to pass a cursory review.

The telephone version of the scam usually involves a male caller whose first language is not English, as evidenced by a heavy accent and trouble with changing tenses in conversation. The caller usually has an unprofessional manner, and many victims have reported that their callers started the conversation by being insulting or abusive, or became so shortly after the conversation began.

In addition to the victims' telephone numbers or electronic mail addresses, the criminals often have pieces of the victims' other identifying information, such as name or address, which they use to make their attempts appear more authentic.

What To Do:

Because these criminals are also involved with identity theft, the TOIG recommends that, if you are contacted by one of them, you delete the electronic mail message or hang-up as soon as you recognize that it is a scam attempt. Do not attempt to elicit

information that can be used against him; do not “play along” just for fun; do not attempt to get the caller to admit that he is a fraud; and do not threaten to report the caller to the authorities. **Terminate contact immediately.**

Particularly with respect to telephone calls, it is important to be aware of the danger of giving away personal information without meaning to. Just by answering the telephone, you have already given the criminal confirmation of your telephone number, your general location (given away by the area code on your telephone number), your sex, your approximate age, and the fact that you are at home during the day/evening. Some of these criminals have a great deal of experience and are adept at a number of forms of “social engineering” that allow them to obtain information that their victims don’t know is useful to identity thieves.

How to Report:

It is not necessary to report a fraud attempt of this sort to the TOIG, which investigates these matters broadly, as part of a task force with other law-enforcement agencies. The TOIG does not investigate or respond to individual reports of, or requests regarding, this kind of consumer fraud.

Anyone who receives a fraudulent electronic mail contact of this sort should consider filing a complaint with the Internet Crime Control Center (ICCC), at www.ic3.gov. The ICCC is a joint partnership between the Federal Bureau of Investigation and the National White Collar Crime Center.

Fraudulent communications purportedly from Internal Revenue Service officials should be reported to the Treasury Inspector General for Tax Administration (TIGTA) at: http://www.treasury.gov/tigta/contact_report_scam.shtml

If the contacts persist, contact your internet or telephone service provider to have the sender blocked.

If you have already provided personal or banking information to one of these criminals, then you should contact your banking institution(s) and/or credit card issuer(s) for assistance in protecting yourself against identity theft. If you have already provided money to one of these criminals, then you should report the crime to your local police force.

Other Resources:

The Federal Trade Commission has set-up a national resource website that provides detailed information to help citizens deter, detect, and defend against identity theft, as well as learn what actions to take if a citizen's identity is stolen:

http://www.ftc.gov/bcp/edu/microsites/idtheft/.

The Financial Fraud Enforcement Task Force offers additional information regarding protecting oneself against various frauds: http://www.stopfraud.gov