Rodney Alexander / Louisiana's 5th District
UNITED STATES CONGRESSMAN

FOR IMMEDIATE RELEASE
March 5, 2008

Contact: Jenni Terry
202/225-8490

Alexander Urges Taxpayers to Heed IRS' Warning of Filing Season Scams

Schemes Target Recipients of Standard, Stimulus Rebates

WASHINGTON, D.C. – With tax season underway, U.S. Rep. Rodney Alexander, R-Quitman, advises residents of the 5th Congressional District to be aware of scams that commonly target citizens expecting tax rebates.

Recently, the Internal Revenue Service (IRS) issued a warning to consumers outlining scams often carried out through telephone or e-mail.

Alexander noted that this year more taxpayers are likely to receive a rebate check as a result of the recently passed Economic Stimulus Package, and it is important to be informed of potential threats.

"Unfortunately, the threat of identity theft is a permanent part of life these days," Alexander said. **"As the tactics used by these criminals are becoming more advanced, we have to keep ourselves educated so that we will not fall victim to their scams."**

If you are a victim of identity theft, please contact one of Rep. Alexander's district offices for assistance. Contact the Monroe office at (318) 322-3500 or the Alexandria office at (318) 445-0818.

Below are key excerpts from the warning issued by the IRS. For more information, call the IRS hotline at 1-800-366-4484 or visit the IRS Web site at http://www.irs.gov.

Rebate Phone Call

At least one scheme using the word "rebate" as part of the lure has been identified. In that scam, consumers receive a phone call from someone identifying himself as an IRS employee. The caller tells the targeted victim that he is eligible for a sizable rebate for filing his taxes early. The caller then states that he needs the target's bank account information for the direct deposit of the rebate. If the target refuses, he is told that he cannot receive the rebate.

This phone call is a scam. No legislation has yet been enacted that would allow the IRS to provide advance payments to taxpayers or that determines the details of those payments. Moreover, the IRS does not force taxpayers to use direct deposit. Those who opt for direct deposit do so by completing the appropriate section of their tax return, with bank routing and account information, when they file; the IRS does not gather the information by telephone.

Refund e-Mail

The IRS has seen several variations of a refund-related bogus e-mail which falsely claims to come from the IRS, tells the recipient that he or she is eligible for a tax refund for a specific amount, and instructs the recipient to click on a link in the e-mail to access a refund claim form. The form asks the recipient to enter personal information that the scamsters can then use to access the e-mail recipient's bank or credit card account.

In a new wrinkle, the current version of the refund scam includes two paragraphs that appear to be directed toward tax-exempt organizations that distribute funds to other organizations or individuals. The e-mail contains the name and supposed signature of the Director of the IRS's Exempt Organizations business division.

This e-mail is a phony. The IRS does not send unsolicited e-mail about tax account matters to individual, business, tax-exempt or other taxpayers. Filing a tax return is the only way to apply for a tax refund; there is no separate application form.

Audit e-Mail

Another new scam brought to IRS attention contains features not seen before by the IRS. Using a technique calculated to get almost anyone's attention, the e-mail notifies the recipient that his or her tax return will be audited. This is the first scam of which the IRS is aware that uses this to get the victim to respond.

Unusual for a scam e-mail, it may contain a salutation in the body addressed to the specific recipient by name. Most scam e-mails seen by the IRS are sent using the same technique used by spammers, in which hundreds of thousands of messages are sent to potential victims based on Internet address. Because of the volume, the typical scam e-mail is not personalized.

This e-mail instructs the recipient to click on links to complete forms with personal and account information, which the scammers will use to commit identity theft. This e-mail is a phony. The IRS does not send unsolicited, tax-account related e-mails to taxpayers.

Changes to Tax Law e-Mail

This bogus e-mail is addressed to businesses, accountants and "Treasury" managers. It instructs them to download information on tax law changes by clicking on a series of links to publications on businesses, estate taxes, excise taxes, exempt organizations and IRAs and other retirement plans. The IRS believes that clicking on a link downloads malware onto the recipient's computer. Malware is malicious code that can take over the victim's computer hard drive, giving someone remote access to the computer, or it could look for passwords and other information and send them to the scamster. There are other types of malware, as well. The urls contained in the link are not legitimate IRS Web addresses.

Paper Check Phone Call

In a current telephone scam, a caller claims to be an IRS employee who is calling because the IRS sent a check to the individual being called. The caller states that because the check has not been cashed, the IRS wants to verify the individual's bank account number. The caller may have a foreign accent.

In reality, the IRS leaves it entirely up to the individual to choose to cash or not cash a paper check. The IRS has no business need to know, and does not ask for, bank account or similar information, except when taxpayers indicate on their tax return that they are opting for the direct electronic deposit of their refund. In that case, however, it is the individual's responsibility to provide the IRS with the correct bank routing and account numbers on the tax return; the IRS does not contact taxpayers to verify the information.

###