INTERNAL REVENUE SERVICE
www.irs.gov

IRS News Release

Media Relations Office **Washington, D.C.** **Tel. 202.622.4000**
For Release: 05/01/02 **Release No: IR-2002-55**

IRS WARNS OF SCHEME TO STEAL IDENTITY AND FINANCIAL DATA

WASHINGTON – The Internal Revenue Service warned today of a fraudulent scheme currently circulating that uses fictitious bank correspondence and IRS forms in an attempt to trick taxpayers into disclosing their personal and banking data. The information fraudulently obtained is then used to steal the taxpayer's identity and bank account deposits.

The IRS has received reports of the scam surfacing from coast-to-coast, including in Maine, New York, Georgia, North Carolina, Texas, California and the state of Washington. Dozens of U.S. and foreign victims have been identified so far.

In this scam, a letter claiming to be from the taxpayer's bank states that the "bank" is updating its records in order to exempt the taxpayer from reporting interest or having tax withheld on interest paid on his or her bank accounts or other financial dealings.

Legally, banks must report interest to the IRS and taxpayers must include it as income.

The "bank" correspondence encloses a phony form that purports to come from the IRS and seeks detailed personal and financial data. The letter urges the recipient to fax the completed form to a specific number within 7 days or lose the reporting and withholding exemption, resulting in withholding of 31% on the account's interest. The scheme promoters then use the faxed information to impersonate the taxpayer and gain access to the taxpayer's finances.

One such phony form is labeled "W-9095, Application Form for Certificate Status/Ownership for Withholding Tax." The form requests personal data frequently used to prove identity, including passport number and mother's maiden name. It also asks for sensitive financial data such as bank account numbers, passwords and PIN numbers that can be used to gain access to the accounts.

The fictitious W-9095 appears to be an attempt to mimic the genuine IRS Form W-9, "Request for Taxpayer Identification Number and Certification." The only personal information a genuine W-9 requests is the name, address and Social Security number or employer identification number of the taxpayer.

Another form used in the scam is Form W-8BEN, "Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding." There is a legitimate IRS Form W-8BEN,

-more-

which is used by banks to ensure that their non-U.S. customers meet the criteria to remain exempt from tax reporting requirements. However, the W-8BEN used by the scam promoters has been altered to ask for personal information much like the W-9095. This altered form targets residents of foreign countries who bank in the United States.

Another totally fictitious IRS form used in this scam is labeled "W-8888." It too asks for information similar to the phony W-9095 and W-8BEN.

The real Forms W-9 and W-8BEN can be found on the IRS's Web site at *www.irs.gov* .

The Treasury Inspector General for Tax Administration investigates a wide variety of offenses, including the misuse of IRS insignia, seals and symbols and identity theft related to tax administration. Taxpayers who have received a fraudulent letter and form should report this to TIGTA by calling the toll-free fraud referral hotline at 1-800-366-4484, faxing a complaint to 202-927-7018 or writing to the TIGTA Hotline, P.O. Box 589, Ben Franklin Station, Washington, D.C. 20044-0589. TIGTA's Web site is located at *www.ustreas.gov/tigta* .

Identify theft is a federal crime under the Identity Theft and Assumption Deterrence Act of 1998. Violations of the Act are investigated by federal agencies such the U.S. Secret Service, the FBI and the Postal Inspection Service and are prosecuted by the Department of Justice. Use of the U.S. mail to commit fraud is another federal crime investigated by the Postal Inspection Service.

Identity thieves can use someone's personal data to:

– Take over his or her financial accounts.
– Run up charges on the victim's existing credit cards.
– Apply for loans, credit cards, services or benefits in the victim's name.
– File fraudulent tax returns.

People who receive the fraudulent letter and form in the mail should immediately contact TIGTA and their financial institution about the attempted fraud. Those who have already been victimized by this scheme should contact the fraud or security department of their creditors, banks and financial institutions, as well as TIGTA and their local police department and postal inspector's office, to report the identity and financial theft.

Additionally, victims should report the identity and financial theft to the fraud units of the 3 credit reporting bureaus:

– Equifax Credit Information Services, Consumer Fraud Division (800-525-6285)
– Experian (888-397-3742)
– Trans Union Fraud Victim Assistance Department (800-680-7289)

A copy of the scam letter and phony W-9095 may be found on the Office of the Comptroller of the Currency's Web site at *www.occ.treas.gov* . Additional information on identity theft, mail fraud and investigative responsibilities may be found on the following Web sites:

- *www.ustreas.gov/tigta*
- *www.usps.com/postalinspectors/fraud/identitytheft*
- *www.consumer.gov/idtheft*
- *www.secretservice.gov/financial_crimes*
- *www.occ.treas.gov*

XXX