GOVERNMENT OF THE DISTRICT OF COLUMBIA

OFFICE OF THE ATTORNEY GENERAL

oag.dc.gov

FOR IMMEDIATE RELEASE: Thursday, March 9, 2017

Contact: Rob Marus, Communications Director: (202) 724-5646; robert.marus@dc.gov
Marrisa Geller, Public Affairs Specialist: (202) 724-5448; marrisa.geller@dc.gov

Attorney General Racine Reminds Residents of 'Seven Scams to Avoid' this Tax Season

As IRS and District Income Tax Filing Deadlines Approach, AG Shares Tips with Residents

WASHINGTON, D. C. – With the filing season for District and federal income tax returns underway, Attorney General Karl A. Racine today cautioned District residents to be on the lookout for fraudulent schemes common during tax season. In particular, he singled out "Seven Scams to Avoid" for the 2017 tax season.

"Our office works year-round to protect hard-working consumers from being scammed, but we increase our efforts during tax season because con artists prey on taxpayers who are sharing important financial information," said Attorney General Racine. **"The best way to avoid these scams is to know the warning signs, which is why we are alerting District residents to seven common tax-season scams."**

If you believe you have been a victim of one of the below tax-season scams, please **call our Consumer Protection Hotline at (202) 442-9828 or send an e-mail to consumer.protection@dc.gov**. You can also learn ways to practical tips to protect yourself from identity theft, phone scams, charity scams, and more by visiting our Office of Consumer protection at oag.dc.gov/ConsumerProtection.

Attorney General Racine's "Seven Scams to Avoid" for the 2017 Tax Season

1. **Phone Fraud**: Taxpayers may receive aggressive and threatening telephone calls from criminals posing as Internal Revenue Service (IRS) agents. The calls often threaten prosecution if the taxpayer does not immediately pay a fine, which can total thousands of dollars. These callers also threaten arrest, deportation, the revocation of licenses, and other negative consequences as a result of purported tax debts. In most cases, if a taxpayer owes back taxes, the IRS does not first contact the taxpayer by phone; rather the IRS will usually first contact those who owe taxes via mail. The IRS also does not

demand immediate payment, cash payments, or ask for credit-card or debit-card numbers over the phone. If you think you owe federal taxes, call the IRS at 1-800-829-1040 to confirm. Visit the IRS website for more information about phone fraud.

2. **Phishing:** Phishing is the practice of using imposter emails or websites to steal personal information. The IRS generally does not first make contact with taxpayers through emails, text messages, or social-media outlets. Consumers should not click on any links in electronic messages claiming to be from the IRS if the message arrived without warning. If you receive a suspicious email or other electronic message claiming to be from the IRS, report it to phishing@irs.gov. Visit the IRS website for more information about phishing.

3. **Identity Theft:** Taxpayers should always be vigilant about identity theft, but particularly during tax season. Criminals sometimes file fraudulent returns using someone else's Social Security number in order to claim their refunds. Visit the Office of the Attorney General's website or the FTC website for more information about identity theft.

4. **Return Preparer Fraud**: While the vast majority of tax professionals provide honest tax-preparation services, some dishonest preparers set up shop during tax-filing season to perpetrate refund fraud—including identity theft and other schemes that defraud taxpayers. Return preparers are a vital part of the U.S. tax system. Legitimate preparers of federal returns should have an IRS Preparer Tax Identification Number (PTIN). Anyone with a valid 2017 PTIN is authorized to prepare federal tax returns. Visit the IRS website for more information about return preparer fraud.

5. **Inflated Refund Claims**: Taxpayers should be wary of any tax preparer who promises outlandishly large refunds. Taxpayers should also avoid any preparer who asks them to sign a blank return, promises a large refund before examining their tax records, or who charges fees based on a percentage of the refund. These kinds of fraudsters often attract victims using flyers, advertisements, phony storefronts, and word-of-mouth via community and religious groups. Visit the IRS website for more information about inflated refund claims.

6. **Fake Charities**: Taxpayers should always be vigilant to avoid organizations masquerading as legitimate charities to attract donations from unsuspecting contributors, but particularly during tax season. Claiming donations to illegitimate charities on a tax refund can lead to serious negative consequences for taxpayers. Before donating to a new charity, take a few extra minutes to check whether it is legitimate. Be wary of charities with names very similar to well-known national organizations; some fake charities use names or websites that intentionally imitate those of legitimate groups. Learn more about charity scams at the Office of the Attorney General website and research a charity online at the Better Business Bureau's Wise Giving Alliance: www.bbb.org/charity/. The IRS website also allows people to find legitimate, qualified charities to which donations may be tax-deductible at https://www.irs.gov/Charities-&-Non-Profits/Search-for-Charities.

7. **W-2 Phishing Scam**: Just like individual taxpayers, District businesses need to be on the lookout for tax-season scams. The W-2 phishing scam uses an imposter email address and the name of a corporate officer to request W-2 information from a company's payroll or human resources department. This phishing scam often requests the information with urgency, collecting an employee's name, date of

birth, social security number, and salary details. If a payroll or human resources employee receives an unusual request from an executive requesting this information, confirm the validity of the email. Visit the IRS website for more information about the W-2 phishing scam.

###