INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.317.4000
www.irs.gov/newsroom | Public Contact: 800.829.1040

IRS and Security Summit Partners Warn of Fake Tax Bill Emails

IR-2016-123, Sept. 22, 2016

WASHINGTON — The Internal Revenue Service and its Security Summit partners today issued an alert to taxpayers and tax professionals to be on guard against fake emails purporting to contain an IRS tax bill related to the Affordable Care Act.

The IRS has received numerous reports around the country of scammers sending a fraudulent version of CP2000 notices for tax year 2015. Generally, the scam involves an email that includes the fake CP2000 as an attachment. The issue has been reported to the Treasury Inspector General for Tax Administration for investigation.

The CP2000 is a notice commonly mailed to taxpayers through the United States Postal Service. It is never sent as part of an email to taxpayers. The indicators are:

- These notices are being sent electronically, even though the IRS does not initiate contact with taxpayers by email or through social media platforms;
- The CP 2000 notices appear to be issued from an Austin, Texas, address;
- The underreported issue is related to the Affordable Care Act (ACA) requesting information regarding 2014 coverage;
- The payment voucher lists the letter number as 105C.

The fraudulent CP2000 notice included a payment request that taxpayers mail a check made out to “I.R.S.” to the “Austin Processing Center” at a Post Office Box address. This is in addition to a “payment” link within the email itself.

IRS impersonation scams take many forms: threatening telephone calls, phishing emails and demanding letters. Learn more at Reporting Phishing and Online Scams.

Taxpayers or tax professionals who receive this scam email should forward it to phishing@irs.gov and then delete it from their email account.

Taxpayers and tax professionals generally can do a keyword search on IRS.gov for any notice they receive. Taxpayers who receive a notice or letter can view explanations and images of common correspondence on IRS.gov at Understanding Your IRS Notice or Letter.

To determine if a CP2000 notice you received in the mail is real, see the Understanding Your CP2000 Notice, which includes an image of a real notice.

A CP2000 is generated by the IRS Automated Underreporter Program when income reported from third-party sources such as an employer does not match the income reported on the tax return. It provides extensive instructions to taxpayers about what to do if they agree or disagree that additional tax is owed.

It also requests that a check be made out to “United States Treasury” if the taxpayer agrees additional tax is owed. Or, if taxpayers are unable to pay, it provides instructions for payment options such as installment payments.

The IRS and its Security Summit partners – the state tax agencies and the private-sector tax industry – are conducting a campaign to raise awareness among taxpayer and tax professionals about increasing their security and becoming familiar with various tax-related scams. Learn more at Taxes. Security. Together. or Protect Your Clients; Protect Yourself.

Taxpayers and tax professional should always beware of any unsolicited email purported to be from the IRS or any unknown source. They should never open an attachment or click on a link within an email sent by sources they do not know.

—30—