IRS warns of fake Affordable Care Act-related tax bill emails

IR 2016-123

IRS and the members of the Security Summit have 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.

Background. Form CP2000 is sent by IRS to a taxpayer when income reported from third-party sources such as an employer does not match the income reported on the taxpayer's tax return. It provides instructions to taxpayers about what to do if they agree or disagree that additional tax is owed. It 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.

In 2015, IRS Commissioner Koskinen convened a Security Summit with chief executive officers and leaders of private sector firms and federal and state tax administrators to discuss emerging threats on identity theft and expand existing collaborative efforts to stop fraud. The Security Summit met again in 2016.

IRS issues a warning. In IR 2016-123, IRS and the Security Summit members are informing taxpayers and tax professionals that IRS has received numerous reports around the country of scammers sending a fraudulent version of CP2000 notices for tax year 2015.

How to identify the scam emails. IRS notes the following characteristics of the scam notices:

- An email that includes the fake CP2000 as an attachment;
- The notice appears to be issued from an Austin, Texas, address;
- The underreported issue is related to the Affordable Care Act requesting information regarding 2014 coverage;
- The payment voucher lists the letter number as 105C;
- The notice includes 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.

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. IRS does not initiate contact with taxpayers by email or through social media platforms.

What taxpayers and tax professionals should do. 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 ”Understanding Your CP2000 Notice,” which includes an image of a real notice.

Taxpayers and tax professionals should be wary of any unsolicited email purported to be from 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.

Other. The issue has been reported to the Treasury Inspector General for Tax Administration for investigation.

IR 2016-123 also contains a reminder that IRS and the Security Summit members are conducting a campaign to raise awareness among taxpayers and tax professionals about increasing their security and becoming familiar with various tax-related scams.