Will the IRS Tax Return Data Breach Impact You?

May 28, 2015

As you no doubt have heard on the news, the IRS recently announced that cyber thieves have gained access to over 100,000 taxpayers' tax return information. According to a number of news sources, that breach has been traced to Russia.

The criminals did not actually gain access to IRS secure databases by hacking into the IRS computer system. Instead, they simply used an online tool provided by the IRS through which taxpayers are able to obtain transcripts of their previously filed tax returns. That service, called "Get Transcript," is available to anyone who, with the correct information, can access an individual's transcripts. The problem is this: the information needed to access "Get Transcript" is readily available from other online sources, which made it easy for the criminals to access a large number of taxpayer accounts.

More than 100,000 taxpayer accounts were breached, while another 100,000 attempts failed, compared to 23 million legitimate taxpayers who were able to successfully download their tax history. It is assumed the criminals' purpose is to obtain taxpayer information needed to file fraudulent tax returns and thus obtain illegitimate refunds.

The IRS has already taken steps to mitigate the damage. The "Get Transcript" service provides two ways to receive a transcript, one online and the other by mail. The online version has been shut down for now and transcripts can only be acquired by mail, which takes up to 10 days.

All taxpayers whose accounts were accessed, and the additional 100,000 accounts to which access was attempted but failed, will be notified very soon. The IRS is offering free credit monitoring and repair services to those who were affected. All 200,000+ accounts will also be flagged so that fraudulent tax returns cannot be filed.

Meanwhile, according to several news services, the Treasury Inspector General, Homeland Security and the FBI have all launched investigations. Moreover, the Senate Finance Committee, which oversees the IRS, will hold a hearing on the data theft.

Is there a lesson to be learned here? Absolutely: limit what information you make available on the Internet and to whom you provide it. Once personal data is online, it is very difficult to remove it. Question everyone's need for any personal information. This is especially true for your SSN, date of birth, bank account numbers, passwords, credit card numbers, etc. Even such things as your mother's maiden name, where you were born and what high school you attended are frequently used to identify you when accessing accounts. Don't post any sensitive data on social media sites and educate your children about the information they post on their social profiles.

If you believe you are at risk due to a lost or stolen purse or wallet, questionable credit card activity or credit report, you should contact the IRS Identity Protection Specialized Unit at 800-908-4490, extension 245 (Monday - Friday, 7 a.m. - 7 p.m. local time; Alaska and Hawaii follow Pacific time). You should also complete and file Form 14039 – IRS Identity Theft Affidavit.

In addition to reporting a theft or possible theft to the IRS, the following actions are recommended:

- Report incidents of identity theft to the Federal Trade Commission at www.consumer.ftc.gov or the FTC Identity Theft hotline at 877-438-4338.
- File a report with the local police.
- Contact the fraud departments of the three major credit bureaus:
  - Equifax – www.equifax.com, 800-525-6285
  - Experian – www.experian.com, 888-397-3742
  - TransUnion – www.transunion.com, 800-680-7289
- Close any accounts that have been tampered with or opened fraudulently.