IRS launches identity theft awareness campaign aimed at tax preparers

James J. Giszczak | Thursday, July 14, 2016

Last year, an unidentified group of hackers launched a massive cyberattack against the IRS and managed to gain access to personal data of more than 700,000 taxpayers. The stolen information included Social Security numbers, birthdates, street addresses and other sensitive data that cyber thieves could use to impersonate a real taxpayer, file a false federal tax return and collect a refund. In the immediate aftermath of this large scale cyber attack, the IRS took steps to improve its own cyber defense systems and to expand its efforts in detecting identity theft tax refund fraud—both internally and externally.

According to a report from the U.S. Treasury Department's Inspector General for Tax Administration, the IRS identified 42,128 tax returns with $227 million claimed in fraudulent refunds, as of March 5, 2016. The report also notes that the IRS prevented the issuance of $180.6 million (79.6 percent) in fraudulent returns and identified 20,224 potentially fraudulent tax returns filed by prisoners, thanks in large part to the wide range of identify-theft filters it had in place.

As part of its external efforts to combat identity theft tax refund fraud, the IRS has partnered with leaders from state tax agencies and executives from the private-sector tax industry to form a united and coordinated front against cyber thieves called the Security Summit. In line with its overall objective—to increase awareness among tax professionals of the threat data theft poses to them and their clients, and the steps they can take to prevent it—the Summit recently launched the "Protect Your Clients; Protect Yourself" campaign. The campaign focuses on educating tax preparers about cyber risks and ensuring they have implemented appropriate security measures to protect their clients' personal information from tax-related identity theft.

Over the course of the campaign, the IRS will issue fact sheets and tips on security, scams and identity theft prevention measures aimed at tax professionals, who are increasingly becoming the targets of cyber attacks. The first fact sheet includes some critical steps to protect taxpayer information and to build client confidence and trust. Some of these critical steps include:

1. Making sure that information is not left unsecured.
2. Requiring strong passwords and periodic password changes (every 60-90 days) on tax-software programs.
3. Ensuring emails that contain taxpayer data are encrypted.
4. Creating security requirements for the entire staff regarding computer information systems, paper records and use of taxpayer data.

5. Restricting access to taxpayer data to authorized users only.

A complete version of the fact sheet can be found here.

To learn more about preventing tax related identity theft, contact one of the data privacy attorneys listed below.

 James J. Giszczak