National Tax Security Awareness Week: Five Steps Data Breach Victims Can Take

IRS Tax Tip 2017-84
November 29, 2017

Every day, data thefts put people's personal and financial information at risk. There are steps that identity theft victims can take to protect their financial accounts, their identities and their tax returns.

This tip is part of National Tax Security Awareness Week. The IRS is partnering with state tax agencies, the tax industry and groups across the country to remind people about the importance of data protection.

Generally, thieves want to use the stolen data as quickly as possible. That may mean selling the data on the Dark Web for use by other criminals. It may also mean the crook tries to withdraw money from bank accounts or charge credit cards. A thief might also try to file a fraudulent tax return using victims' names for a refund.

People who are the victim of a data breach should consider these five steps to help protect their sensitive information that can be used on a tax return:

- If possible, the victim should try to determine what information the thieves compromised. Victims can try to find out if the criminals accessed emails and passwords, or more sensitive data such as name and Social Security number.

- Breached companies often offer credit monitoring services to victims. Victims should consider taking advantage of these offers.

- Victims should place a freeze on credit accounts to prevent access to credit records. There may be a fee that varies by state. At a minimum, victims should place a fraud alert on their credit accounts by contacting one of the three major credit bureaus. A fraud alert on credit records is not as secure as a freeze, but a fraud alert is free.

- Victims should reset passwords on online accounts. It is especially important to reset passwords of financial sites, email and social media accounts. Some experts recommend at least 10-digit passwords mixing letters, numbers and special characters. People should use different passwords for each account, using a password manager or password app if necessary.

- People should use multi-factor authentication when available. Some financial institutions, email providers and social media sites allow users to set their accounts for multi-factor authentication. This means users may need a security code, usually sent as a text to their mobile phone, in addition to a username and password.

More Information:

Taxes. Security. Together
Protect Your Clients; Protect Yourself
Don't Take the Bait