INTERNAL REVENUE SERVICE
IRS Fact Sheet

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

Tax Professionals: Protect Your Clients; Protect Yourself from Identity Theft

FS-2016-23, July 2016

The Security Summit, the partnership between the IRS, state tax agencies and the tax community formed to combat identity theft, recently announced it expanded its public awareness campaign on data security to include tax professionals.

The "Protect Your Clients; Protect Yourself" campaign is intended to raise awareness among tax professionals on their responsibilities and the common sense steps they can take to protect their clients from identity theft and to protect their businesses.

Because of the sensitive client data held by tax professionals, cybercriminals increasingly are targeting the tax preparation community, using a variety of tactics from remote computer takeovers to phishing scams.

How are Tax Preparers Impacted? Identity thieves are a formidable enemy. Data breaches are increasing in number and scope, increasing the potential for stolen identity information to be used to file tax returns. As a tax preparer, you play a critical role in protecting taxpayer data.

What is my role as a preparer? It is a legal responsibility of businesses and individuals that maintain, share, transmit, or store taxpayer data to have safeguards in place to protect client information. Taxpayer data is defined as **any** information obtained or used in the preparation of a tax return.

What Can I Do? Data security includes all aspects of your business. Review your administrative practices, facility protection, computer security, personnel & information systems.

Read the complete IRS Publication 4557, Safeguarding Taxpayer Data, for a more comprehensive view including tips and links to additional information.

Critical Steps:

- Assure that taxpayer data, including data left on hardware and media, is never left unsecured
- Securely dispose of taxpayer information
- Require strong passwords (numbers, symbols, upper & lowercase) on all computers and tax software programs
- Require periodic password changes every 60 – 90 days
- Store taxpayer data in secure systems and encrypt information when transmitting across networks

- Ensure that e-mail being sent or received, that contains taxpayer data, is encrypted and secure
- Make sure paper documents, computer disks, flash drives and other media are kept in a secure location and restrict access to authorized users only
- Use caution when allowing or granting remote access to internal networks containing sensitive data
- Terminate access to taxpayer information for anyone who is no longer employed by your business
- Create security requirements for your entire staff regarding computer information systems, paper records and use of taxpayer data
- Provide periodic training to update staff members on any changes and ensure compliance
- Protect your facilities from unauthorized access and potential dangers
- Create a plan on required steps to notify taxpayers should you be the victim of any data breach or theft

Additional Considerations:

- Complete a risk assessment to identify risk and potential impacts of unauthorized access
- Write and follow an Information Security plan
- Consider performing background checks and screen individuals before granting access to taxpayer information

Putting safeguards in place to protect taxpayer data helps prevent fraud and identity theft and enhances customer confidence and trust. These safeguards will help you:

1. Preserve the confidentiality and privacy of taxpayer data by restricting access and disclosure
2. Protect the integrity of taxpayer data by preventing improper or unauthorized modification or destruction; and
3. Maintain the availability of taxpayer data by providing timely and reliable access and data recovery.

—30—