THE TAXBOOK News
Release Date: 11/21/16

Identity Theft is the Hot Topic at Fall Tax Seminars

Cross References

- FS-2016-23
- IR-2016-96
- IRS Pub. 4557, *Safeguarding Taxpayer Data*

With the fall tax seminar season in full swing, the number one topic discussed this year is identity theft. The sensitive client data held by tax professionals on their computers is attracting cybercriminals who are targeting the tax preparation community, using a variety of tactics in an attempt to steal the identity of taxpayers. Data breaches are increasing in number and scope, increasing the potential for stolen identity information to be used to file tax returns. Tax preparers play a critical role in protecting taxpayer data.

What can tax preparers do? Data security includes all aspects of a tax preparer's business. A tax preparer should review his or her administrative practices, facility protection, computer security, personnel & information systems. IRS Pub. 4557, *Safeguarding Taxpayer Data,* suggests the following procedures that tax preparers should implement to protect client data:

- 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 and lowercase) on all computers and tax software programs.
- Require periodic password changes every 60 to 90 days.
- Store taxpayer data in secure systems and encrypt information when transmitting across networks.
- Ensure that email 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 the tax preparer's business.
- Create security requirements for the tax preparer's 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 facilities from unauthorized access and potential dangers.
- Create a plan on required steps to notify taxpayers if there is any data breach or theft.

- 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.

Blunt advice from a tax seminar speaker. A tax seminar speaker recently told his audience that he has been the subject of several e-file audits over the years. Each time his e-file procedures were found to be in accordance with IRS rules and regulations. He questioned the auditor why he was being targeted multiple times. The auditor said because he has a big mouth. This was not meant as an insult. The auditor acknowledged that he was in compliance with e-file procedures. The real reason for the multiple audits was because as a tax seminar speaker, he would relay information to the tax preparer community in a way that the IRS cannot. The auditor said that the primary source for information stolen by identity thieves is from tax professionals with unsecure computer and data systems. With this in mind, the tax seminar speaker provided the following additional advice for how to prevent identity thieves from stealing client data from tax preparers:

- Encrypt all hard drives and emails. A password to log into your computer is not good enough because if your computer is stolen, the hard drive can be removed and plugged into another computer, bypassing the password that you use to log into your computer. This requires special encryption software to be installed on all hard drives that store client data.
- Turn off all computers every night. Leaving a computer on and plugged into the internet is like putting a sign on your front door saying the door is unlocked and nobody is at home. Please come in and help yourself to all of my stuff. Turning off the computer when not in use prevents identity thieves from hacking into your computer and remotely downloading data from your computer.
- Reboot your computer before lunch or appointments. Do not log back in until after you return.
- Use special password protection software to prevent identity thieves from breaking through your passwords.
- Use anti-virus, anti-ransomware, anti-phishing, anti-malware, and secure browsing software on all computers. Anti-virus protection software by itself is not good enough to defend against all types of e-threats.
- Physically destroy paper and electronic data. This can include shredding or burning paper documents, as well has drilling holes in an old hard drive that is no longer in use. Deleting data from a hard drive does not remove the data. The hard drive needs to be physically destroyed to prevent an identity thieve from accessing the data on it.
- Implement written "no-click" and computer use policies. Clicking on an email attachment is a common way for identity thieves to install ransomware and malware on your computer and access your data. Even if you think you know the source of the email, do not click on links or open attachments. Require clients to either physically mail the data, drop it off in your office, or use a cloud service to upload and download sensitive data such as W-2s, 1099s, etc.

- **Do not use smart phones, tablets, or laptop computers to remotely access your office computer. If you can remotely access sensitive data on your computer, so can identity thieves.**
- **Utilize sterile office operations and interviews. This means clients should not be allowed to see or have access to other client files. Do not have piles of work in progress on the floor in your office during interviews with other clients. If your front desk receptionist makes copies or scans client documents during business hours, do not let him or her leave the room while clients are sitting in the waiting room. Client data should never be left out unattended. If you cannot clean up your office and remove client files from view prior to a client interview, then use a conference room with no files in it to interview your clients.**