Bloomberg Tax

Tax Management Memorandum™

The Cybersecurity Threat, Burden, and Role of Tax Practitioners

By Gary Wells, Esq., CPA[*]

Tax practitioners have learned that they possess something that a new breed of criminals, namely cybercriminals, desire—information. The storage of taxpayer data in the Cloud and on open network systems provides a competitive advantage to tax practitioners to access client information quickly and transmit data efficiently to the Internal Revenue Service and other state authorities on behalf of their clients. With this benefit comes a heightened risk that unauthorized individuals, especially cybercriminals, will have greater opportunity to intercept or steal the same information for their own unlawful devices. In calendar year 2016, it was estimated that between $1.68 billion to $2.31 billion of federal income tax refunds reached identity thieves (including cybercriminals) unabated by defensive measures adopted by the IRS to stymie their illicit efforts. An estimated 740,000 to 810,000 tax returns were compromised.[1]

Noted bank robber, Willie Sutton, offered a simple explanation of why he robbed banks by saying "That's where the money is."[2] Unlike in the days of Willie Sutton, today valuable items are stored in places other than banks, and cybercriminals may subvert valuable client data and utilize it to enter into illicit transactions, including filing unauthorized tax returns. The cybercriminals often target tax practitioners because they possess information such as client names, addresses, birth dates, social security numbers, and bank account information—the basic data elements necessary to file a tax return. Collectively the information pursued is commonly referred to as personally identifiable information (PII). After acquiring PII from businesses via confederates with access to such information, either by purchase in the dark web marketplace for stolen data or infiltrating a tax practitioner's information network, a cybercriminal may impersonate a known tax practitioner to file unauthorized returns. The stolen information may come from multiple places, including tax practitioners, and the cybercriminal may use the information for a number of illicit purposes, e.g., open new credit card accounts, securing mortgages, and filing tax returns, among others.[3] The IRS refers to the filing of unauthorized tax returns as identity theft tax return fraud (IDTTRF).[4] This article focuses primarily upon the specific class of unauthorized tax returns resulting from cyberattacks upon tax practitioners. The following table highlights several methods that identity thieves employ to acquire the necessary information from tax practitioners that lead to instances of IDTTRF.[5]

---

[*] Mr. Wells is Of Counsel with the BILTgroup (DC) an international tax and federal/state controversy law firm, and Gordon Rees (New Jersey), a national law firm. He specializes in taxation of financial institutions, international tax, information reporting and tax controversy matters. He has published previously on tax matters germane to financial institutions and IRS controversy issues and may be reached at gwells@BILTgroup.net and gwells@grsm.com.

[1] TIGTA, *Partnership with State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft*, p. 4, Fig. 1 (Dec. 27, 2018).

[2] Robert M. Yoder, *Someday They'll Get Slick Willie Sutton*, The Saturday Evening Post, Vol. 223, Issue 30 (Jan. 20, 1951).

[3] Jay Weaver, *These South Florida scammers stole identities, then millions from the IRS*, Miami Herald (Sept. 11, 2018); General Accounting Office, *Identity Theft and Tax Fraud—IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, GAO-16-508, pp. 4-5 (May 2016).

[4] While IDTTRF injures individuals, the same types of unauthorized actions may cause businesses to suffer a loss as well. However, this article focuses on tax practitioners' services offered to individuals and defenses erected to stymie cybercriminals and protect the underlying client data. Nonetheless, the defenses to protect individual clients should protect business clients as well.

[5] IRS Pub. 4557, *Safeguarding Taxpayer Data, A Guide for Your Business*, pp. 5, 18; IR-2018-157, *Tax Security 101: Security Summit reminds tax professional to beware of spear fishing emails* (July 31, 2018).

Common method to gain access to client data	Definition	Weakness exploited	Defenses
Malware	Introduction of software to practitioner's computer system designed to damage network or perform unwanted actions. May come in the form of a virus, ransomware, or spyware.	• Unguarded use of the internet by employees may lead to the introduction of software onto the user's computer or the network. • Sometimes it is offered as free software.	• Use anti-virus, anti-spyware, and utilize drive encryption. • Never select ''security software'' from pop-up advertisement. Select setting for security software to update automatically.
Spear phishing	Email sent by criminal that demonstrates that criminal has researched target in advance of sending email.	• Email appears to originate from trusted source with urgent demand for action **or** simple request (click on embedded link) seems reasonable on its face • Human desire to help and sometimes gullible nature of recipient	• Use separate personal and business email accounts • Protect email with strong passwords and multi-factor authentication • Install an anti-phishing toolbar, often included in many security software products • Use security software to defend against malware and scan emails for viruses
Hacking	Criminal may seek to gain unauthorized access to network via various automated procedures, including known vulnerability scanner, password cracking, and other methods	• Lax control over software updates due to lack of timeliness • Easy to guess passwords	• Ensure timely security and network software updates • Ensure user passwords are tough to guess

During the summer and fall of 2018, the IRS communicated a great deal of advice and guidance concerning its expectations as to what tax practitioners need to do to guard against IDTTRF. For this reason, as well as protecting their livelihood, tax practitioners need to exercise heightened vigilance and defend the valuable client information they acquire via their professional practice from unauthorized persons who may attempt to exploit the information. Like the most wanted person posters in Willie Sutton's day, the IRS has published what the tax practitioner should be on the lookout for.[6] These public announcements highlight the cybersecurity role that the IRS expects tax practitioners to perform in defending the integrity of the tax system.

Many consider the term ''cybersecurity'' and ''information security'' synonymous. However, cybersecurity comprises only a subsection of information security, which, as broadly defined, relates to ''[t]he protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.''[7] Besides cybersecurity, information security includes also physical security, personnel security, contingency planning and disaster recovery, operational security, and privacy.[8] Many of the same safeguard principles, introduced later, apply to each, but this article focuses primarily on cybersecurity.

CYBERCRIMINALS ADAPT TO A CHANGING ENVIRONMENT

The cybercriminals have evolved, adapted, and specialized in infiltrating electronic devices and exploiting the information stored therein. Additionally, the criminals have refined both who they target and how they pursue their ill-gotten gains. Bank robber Willie Sutton surreptitiously entered financial institutions often in disguise as a telegram messenger or postal delivery person, which helped his entry go unnoticed by passersby, especially before the bank's opening hours. This combination of guile and timing helped to ensure his efforts would encounter fewer obstacles and di-

[6] See generally for a list of recent cybersecurity announcements, IRS, National Tax Security Awareness Week 2018.

[7] Celia Paulsen and Patricia Toth, *Small Business Information Security: The Fundamentals*, National Institute of Standards and Technology, p. 2 (Nov. 2016).

[8] *Id.* at p. 3. For the sake of completeness, the following definitions apply to each of the other subsections of information security. ''Physical security'' concerns the protection of property and may involve door looks and fences. ''Personnel security'' concerns verification that employees are qualified to perform tasks assigned and may involve background checks. ''Contingency planning and disaster recovery'' concerns management's time estimate to return normal operations after an incident and the associated processes to ensure such incident. ''Operational security'' concerns the steps necessary to protect business plans and processes. ''Privacy'' concerns the business requirement to protect client and employee personal information.

ISSN 0148-8295

minished the chance of immediate foiling his plot or capture. Today, con artists employ the same approach to avoid detection and seek out those targets that they consider soft (weaker perceived defenses and lower detection rates). Indeed, the IRS itself formerly held the position as the primary target of con artists that would among other ruses submit fictitious earned income credit returns. A number of changes to the law and IRS operating procedures have lessened the success in perpetrating this fraud, including additional due diligence requirements and authentication protocols before the refund may be issued.[9] Nonetheless, the fraudsters continue to adapt to the increased barriers by trying, among other actions, to impersonate the IRS by sending emails to taxpayers trying to entice them to open documents containing malware in which they may unwittingly cause the exposure of all of their computer-stored documents and financial accounts. The information exposed may allow the fraudster to file an unauthorized tax return, IDTTRF, and/or attack tax practitioners' systems to gather the same information for many clients.[10] Additionally, the GAO has advocated additional procedures to enhance authentication before the IRS may share taxpayer data with taxpayers themselves and/or their designees.

On several occasions, the IRS has requested that Congress take incremental action to impose requirements on the tax practitioner community to address certain tax items before signing a tax return containing either an earned income tax credit (EITC), additional child tax credit, and American Opportunity Tax Credit (AOTC) via the preparation of a due diligence tax checklist.[11] The statutory requirement imposes a penalty upon a tax practitioner that does not complete the due diligence tax checklist of at least $500 per occurrence under §6695(g).[12] Formerly, the original checklist (Form 8867, Paid Preparer's Due Diligence Checklist) that was issued in 1997 concerned only the EITC. The due diligence requirement for the AOTC claims was enacted in 2015. These countermeasures inhibited cybercriminals' ability to exploit the EITC, and subsequently the AOTC, benefit for their own devices and placed more responsibility on tax practitioners to police claims they prepared and not facilitate claims that contained indicia of fraud.[13] In 2012, the IRS tightened its own internal review of taxpayer refunds and took substantive steps, such as instituting additional validation protocols and procedures to assess each refund return's fraud characteristics before issuing a refund.[14]

As new defenses are erected that mitigate specific fraud schemes, cybercriminals develop new ruses or avenues that attack different participants in the tax return preparation process that may offer an easier path to success—the weakest link in the data security chain. The fact that cybercriminals are willing to file unauthorized tax returns populated with information gleaned from infiltrating tax practitioner computer systems marks an astounding development in the lengths that cybercriminals will pursue to accomplish IDTTRF and unjustly enrich their coffers.

TAX PRACTITIONERS PROVIDE A TARGET-RICH POPULATION TO CYBERCRIMINALS

During Willie Sutton's heydays in the late 1930s, the United States had approximately 17,000 federally-insured bank offices that served as tempting targets for stealing cash. The cybercriminals of today may ply their trade on an exponentially larger population of targets. According to the IRS, there are over three-quarters of a million tax preparers that help file approximately 79.3 million of the estimated 152.6 million total federal individual income tax returns during the calendar year 2018 filing season.[15] The large numbers of returns and PII contained therein that tax practitioners possess present a tempting target for cybercriminals. The following table demonstrates the sheer volume of identity theft and the progress made by the IRS to intercept the same.[16]

---

[9] Taxpayer Relief Act of 1997, Pub. L. No. 105-34, §1085, introduced new §6695(g)—Failure To Be Diligent in Determining Eligibility for Earned Income Credit; Government Accountability Office, *Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts*, GAO-18-418 (June 22, 2018). All section references are to the Internal Revenue Code of 1986, as amended (Code), or the Treasury regulations thereunder, unless otherwise indicated.

[10] IR-2018-226, *IRS warns of "Tax Transcript" email scam: dangers to business networks* (Nov. 19, 2018); IRS Pub. 4557, Safeguarding Taxpayer Data: A Guide for your Business, p. 18.

[11] Protecting Americans from Tax Hikes Act (PATH ACT), Pub. L. No. 114–113, div. Q, title II, §207(a), codified as §6695(g), which expanded the due diligence tax checklist use to tax benefits other than earned income tax credit.

[12] See also §6695(h), which authorizes an inflation adjustment for the penalty. The 2017 penalty amounts to $510, and for returns filed after 2018, the infraction amount per instance equals $520, per Rev. Proc. 2017-58, §3.48.

[13] The Taxpayer Relief Act of 1997, Pub. L. No. 105-34, §1085, introduced new §6695(g), Failure To Be Diligent in Determining Eligibility for Earned Income Credit.

[14] TIGTA, *Some Tax Returns Selected for Fraud Screening Did Not Have Refunds Held and Required Notifications Were Not Always Sent to Taxpayers*, p. 1 (Mar. 27, 2018).

[15] IRS Pub. 6186, Calendar Year Projections for the United States and IRS Campuses: 2018-2025—2018 Update, Table 2; IRS, Return Preparer Office Federal Tax Return Preparer Statistics.

[16] IR-2018-21, *Key IRS Identity Theft Indicators Continue Dramatic Decline in 2017; Security Summit Marks 2017 Progress*

ISSN 0148-8295

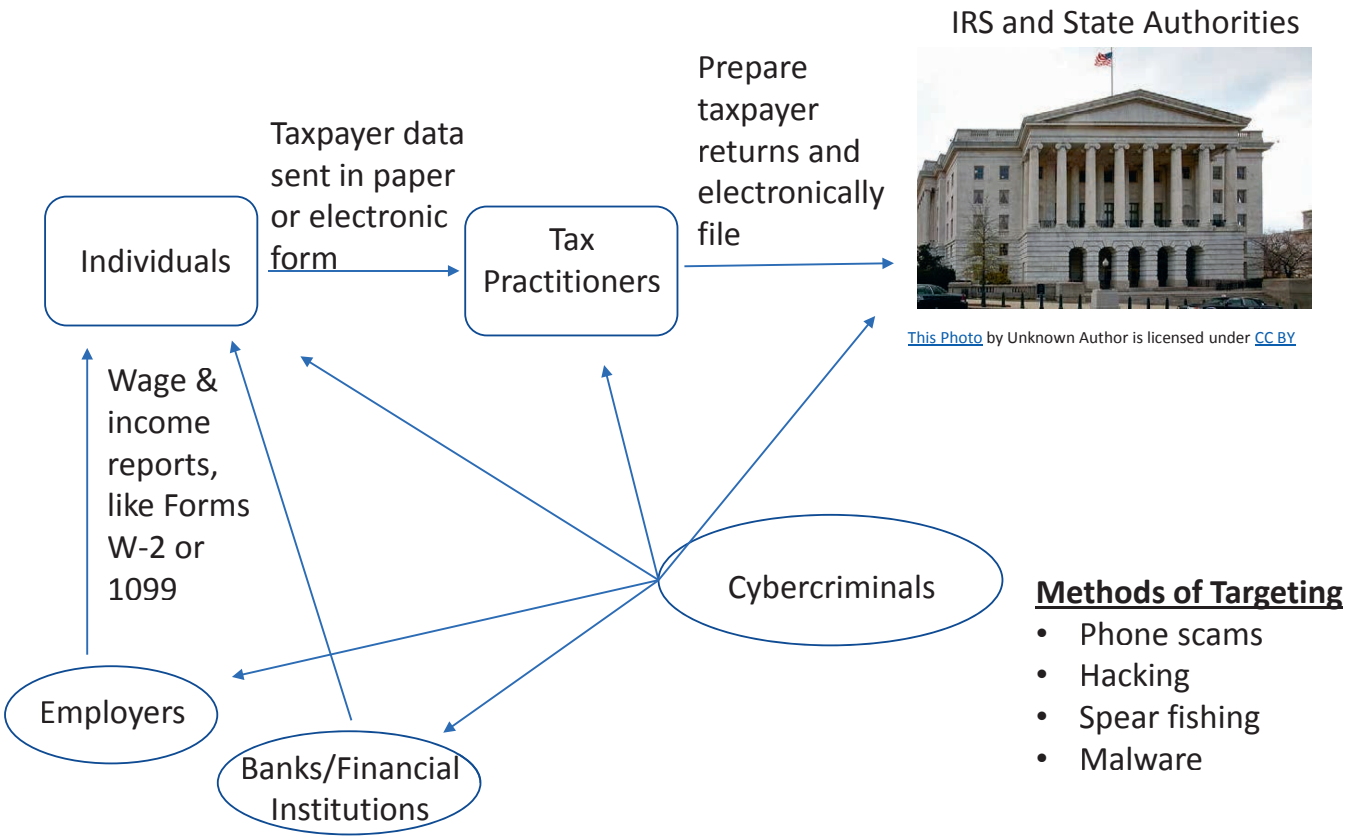
Table 1 – Recognized Volume and Extent of IDTTRF			
Calendar year the Return Received	**Amount of Returns with Confirmed Identity Theft**	**Amount of Refunds Protected**	**Average Refund Claim for Confirmed Identity Theft**
2015	1,400,000	$8.7 billion	$6,214.29
2016	883,000	$6.4 billion	$7,248.02
2017	597,000	$6.0 billion	$10,050.25

While the number of tainted returns and the total refund amounts involved indicate a positive directional trend, based on the IRS efforts (57% percentage decline in identity theft over the three-year period (2015 to 2017)), the sheer number of returns reviewed and the size of the potential loss to the Treasury associated with unauthorized refunds demands an ongoing, robust response by the IRS and the tax community. The IRS has strengthened its defenses via introduction of authentication items before issuing refunds to individuals, e.g., use of prior year adjusted gross income and personal identification numbers, along with other protections.[17] These additional items increase the need of cybercriminals to capture more detailed personal data to try to ensure that they may perpetrate fraud. As noted, the IRS and other authorities have discovered that cybercriminals have begun to target tax professionals, human resource departments, and other places that may hold financial data, including Form W-2 data to bridge the new refund data elements to continue to impersonate actual taxpayers. See Figure 1 for a diagram of the basic electronic income tax return process and the potential sources of actionable information for cybercriminals.

Against Identity Theft (Feb. 8, 2018); IRS Pub. 3415, Electronic Tax Administration Advisory Committee Annual Report to Congress, p. 3.

[17] IRS Pub. 3415, p. 41.

Figure 1 – Individual Income Tax Return Process Participants



This Photo by Unknown Author is licensed under CC BY

ISSN 0148-8295

INTRODUCTION OF SECURITY SUMMIT

In this challenging environment, the mandated development and proliferation of electronic filing offers cybercriminals a steady, tempting opportunity to steal from the Treasury without the need to physically enter the United States via internet access. While Willie Sutton tried to inconspicuously enter banks to delay recognition and detection, cybercriminals try to accomplish their theft with a number of keystrokes that may go undetected until well after the theft has been completed. The electronic refund process, with its goal of faster processing and response times, incentivizes the IRS to claim it completes 90% of its refunds within 21 days.[18] However, the faster refund timeframes increases the potential that the IRS may process refunds for new undetected schemes devised by cybercriminals before the scheme's discovery and after the refunds have been forwarded via direct deposit and out of reach of the IRS.[19] Facing this daunting prospect, the IRS and the tax community recognized the need to collaborate more closely on security issues and the battle against IDTTRF.

Acknowledging the pernicious nature of cybercriminals and their potential future mayhem, the IRS enlisted the active participation of tax practitioners to combat identity theft and protect taxpayer data from other cybercriminal ruses. In March 2015, a number of tax industry stakeholders joined together with the IRS to form the Security Summit. The Security Summit defines its mission as defending the integrity of the tax processing system and thereby protecting taxpayers from identity theft. The IRS recognized the problem surrounding the need to enhance client data protections and formed the Security Summit to bring together knowledgeable stakeholders, including senior IRS personnel, state tax authorities, and tax industry members such as leaders of tax preparation firms, tax software companies, and tax financial product processors.[20] The Security Summit followed the Electronic Tax Administration Advisory Committee (ETAAC)recommendation that tax professionals need to enhance their own system safeguards to decrease the risk of falling victim or being further susceptible to security attacks. In 2016, ETAAC had expanded its mission to include combatting identity theft.

Clearly, the more secure the data, the less likely a refund payment may later be shown to be fraudulent in nature, i.e., IDTTRF. While the IRS wants tax practitioners to act as a pillar in defending the integrity of the tax system against fraud, most tax practitioners do not possess the same resources in terms of information technology personnel and expertise as the IRS. Nonetheless, the IRS has outlined the enhanced security role each tax practitioner must play in the tax ecosystem to avoid running afoul of the IRS expectations and avoid potential censure by the IRS, such as denying tax practitioner access to future electronic filing.[21] Interestingly enough, tax practitioners may discover that cybercriminals have utilized either their EFIN or PTIN , thereby compromising them, and as a consequence the IRS may classify the affected tax practitioner as a fraud indicatorso that in the future, their returns will receive special screening from the IRS.

As noted in Table 1 above, the IRS has quantified its success in combatting identity theft over the last two tax return processing years. However, the extent of the problem facing the IRS in both terms of numbers and persistence should justify the continued vigilance by all tax return participants, including taxpayers and tax practitioners.

WHAT NEXT? SECURITY SUMMIT OUTLINES NEW PLAN

To combat the perceived vulnerabilities and tenacious nature of the cybercriminal population, the Security Summit issued public guidance in the form of a 10-part series to tax practitioners on how to protect the information that clients share in the process of receiving tax return preparation services and alert them to resources that may assist them in combatting fraudulent returns, i.e., an unauthorized tax return filed without the consent of the taxpayer, based on information stolen from a tax practitioner. The breadth of the series showed the important role tax practitioners play and the threat that cybercriminals may have on the tax return process to the detriment of the taxpayers, tax preparers, and the taxing authorities.

What Is the Problem?

Tax firms of all sizes face recurrent threats from cybercriminals that seek to intercept detailed financial information from their systems and convert that information into an unauthorized filed tax return with a tax

---

[18] IRS Pub. 2043, IRS Refund Information Guidelines for the Tax Preparation Community.

[19] The IRS has enlisted the financial industry in its fight against identity theft to recover refunds from bank accounts. *See generally,* IR-2018-21.

[20] IRS Pub. 3415.

[21] There is an open question whether the IRS may deny electronic filing access to tax practitioners serving individuals under its regulatory and enforcement powers. IRS Pub. 3415, pp. 21-22. The IRS continues to remind tax practitioners in public statements that it has the power to deny tax practitioner access to its electronic filing system as elaborated in Rev. Proc. 2007-40. IR-2018-75, *Tax Security 101: Security Summit Reminds professional tax preparers of data security requirements* (Aug. 28, 2018).

ISSN 0148-8295

refund funneled back to the criminal enterprise. The threats take a number of different forms that have different impacts on tax practitioners.

Several notable cases received publicity in Miami in 2018 where criminal groups committed IDTTRF by either seeking large average refunds amounts ($130,000 to $170,000) or filed large number of returns with smaller average refund amounts (1,000 returns with refund amounts sought totalling $7 million).[22] While the IRS broke up both rings, it did pay out large amounts before discovering the fraud, i.e., $4.3 million and $1.5 million, respectively. While these two threats were effectively confronted and prosecuted, the IRS seemingly has fewer tools to confront the same threats that originate across borders. For this reason, the IRS and the Security Summit recognize the need to fortify the defenses of all participants in the tax return process, including tax practitioners.

10-Part Steps or Deputizing Tax Practitioners as IRS Security Apparatus—the Burden

The IRS has issued two publications that address basic security steps encouraged by the Security Summit partners for tax professionals. The IRS considers these security steps, coupled with a sound security plan, to safeguard systems and taxpayer data. IRS Pub. 5293 reminds tax professionals that they must under adequately fulfill their security obligations and act to protect taxpayer data from theft and unauthorized disclosure. This publication recommends that tax professionals read IRS Pub. 4557, Safeguarding Taxpayer Data, and review the National Institute of Standards and Technology's (NIST's) Small Business Information Security—The Fundamentals.

NIST, a branch of the Commerce Department, offers a comprehensive information security framework to private entities. The framework, a voluntary standards-based system that includes best practices, takes several tailored versions that concern different types of entities, but an important goal of the framework itself concerns reducing cybersecurity risk and protecting data.[23] Additionally, NIST has also provided an overview framework to small businesses to help secure its data as well. The security framework concerns the application of five principles to better secure data: identify, protect, detect, respond, and recover.[24] Secure data is vitally important to all businesses, including tax practitioners, because of the high cost associated with remediating lost or compromised data. While a recent study highlighted in the case of large breaches (1 million or more records compromised), a significant cost (one-third of total costs) was attributed to loss of business.[25] Many small businesses, including tax practitioners, will not suffer a large breach due to their smaller amount of data stored, however, a potential loss of one-third of their business would prove devastating. Tax practitioners should look to third-party security consultants for the application and review of the five principles.

A survey of the small and medium-size businesses that suffered a breach provides an average total financial impact associated with the breach of $117,000, and a loss to the enterprise of $1.3 million.[26] Clearly, the costs can be significant and actual costs may differ over the average reported by the surveys. Another harm measure concerns the total average cost per breached record of $148.[27] All of these different measures document the potential significant costs incurred as a result of a breach occurs that justifies taking proactive steps to protect the data.

A tax practitioner that decides to take action and try to limit the potential for future breaches may not have a clear plan of action, especially if they have not either engaged security professionals to check their security procedures previously or possess a cybersecurity background. However, IRS Pub. 4557 offers the initial steps that tax professionals should understand and take to achieve the NIST goal of safeguarding the tax practitioner's client information. The NIST framework provides a starting point and action items that incorporate the NIST small business general principles.[28] The basic steps contained in Pub. 4557 and the broader apparent NIST principle served are listed in the following table:[29]

---

[22] Jay Weaver, *These South Florida scammers stole identities, then millions from the IRS*, Miami Herald (Sept. 11, 2018).

[23] *See generally*, NIST, Framework for Improving Critical Infrastructure Cybersecurity, (April 16, 2018).

[24] *See generally*, Celia Paulsen and Patricia Toth, *Small Business Information Security: The Fundamentals*, National Institute of Standards and Technology, p. 2 (Nov. 2016).

[25] 2018 Cost of a Data Breach Study, Global Overview, Ponemon Institute (July 2018).

[26] Small and medium size businesses comprise between 50 and 999 employees and an enterprise has at least 1,000 employees. Kaspersky Lab, *IT Security: Cost center or strategic investment?*, p. 6 (2018).

[27] 2018 Cost of a Data Breach Study, p. 3.

[28] *Compare*, IRS Pub. 5293, Protect Your Clients; Protect Yourself—Data Security Resource Guide for Tax Professionals; Paulsen and Toth, *Small Business Information Security: The Fundamentals*.

[29] IR-2018-147, *Tax Security 101-IRS, Security Summit partners launch new awareness campaign; Urge tax professionals to step up protections for client data* (July 10, 2018); IRS Pub. 4557.

ISSN 0148-8295

Table 2	
Basic Security Steps	**Parallel NIST Guiding Principle**
Learn to recognize phishing emails	Identify and Protect
Create a data security plan	Protect
Review internal controls for your business	Protect and Detect
Report any data theft or loss to the assigned IRS Stakeholder Liaison and other authorities	Respond
Remain connected to IRS through various subscriptions services	Identify

Importance of a Security Plan

While each basic step enhances the environment that leads to a secure data environment, an important requirement to lower the cybersecurity risk concerns the creation of a security plan that helps document and substantiate the review undertaken by the tax practitioner of the internal controls surrounding customer data. IRS Pub. 4557 contains six categories of basic steps that tax practitioners should follow to ensure their basic security plan will safeguard taxpayer data and help avoid a significant intrusion. Table 3, below, lists the categories, termed the ''Security Six,''[30] and the steps that ensure a stronger security plan and outline internal control practices. The IRS wants tax preparers to know and remain aware as to three principal matters when developing such a plan, including:[31]

1. Define the plan requirements

- Tailor plan to the tax preparer's practice size and complexity with an understanding of the customer information possessed and its inherent sensitivity
- Regularly monitor and test, evaluate, and adjust current safeguards to meet new and emerging security needs and changes to tax practice or operations

2. Designate one or more employees to administer the plan

3. In the case of service providers that deliver service on behalf of clients

- Ensure they also maintain safeguards and handle customer information appropriately
- Insert security requirements into service contracts, and
- Make ability to conform to plan a selection criterion in evaluation of service providers

Five of the six steps from the Security Six are highlighted in the following table, the remaining item not mentioned in the table relates to the preparation of a written data security plan.[32]

[30] IR-2018-150, *Tax Security 101-IRS, Security Summit outlines 'Security Six' basic safeguards for tax professionals' computers and email* (July 17, 2018).

[31] IR-2018-151, *Tips for tax preparers on how to create a data security plan* (Sept. 27, 2018).

[32] IR-2018-150. *See also* IRS Pub. 4557.

ISSN 0148-8295

Table 3					
IRS Pub. 4557 - Safeguarding Taxpayer Data					
Utilize Security Software	**Create Strong Passwords**	**Insure Secure Wireless Network**	**Protect Stored Client Data**	**Remain Vigilant**	**Report Data Loss to IRS and the States**
• **Anti-virus**, • Anti-spyware, • **Firewall**, and • **Drive Encryption**	• Minimum of eight characters • Use combination letters, numbers, and symbols • Choose phrases over personal information or common password • Change default and temporary passwords immediately • Do not reuse passwords • Do not use email address as username • Store passwords in secure location • Use a password manager to track passwords • ***When available, use a multi-factor(two or more)authentication process for returning users***	• Change default admin password of wireless router to a unique password • Reduce wireless range to avoid broadcasting farther than needed • Make sure router name does not contain personally identifiable information, like name of business • Use Wi-Fi Protected Access (WPA-2) with Advanced Encryption Standard (AES) for encryption • Do not use Wired-Equivalent Privacy (WEP) to connect computers to the router because WEP is not considered secure • Do not access business email or sensitive documents with the use of public wi-fi	• **Back-up encrypted files to external hard drives or to the Cloud** • Avoid attaching USB drives and external drives with client data to public computers • Avoid installing unnecessary software or applications to the business network and stay away from ''free software''; download software or applications from official websites • Perform an inventory of devices which hold or store client data • Limit or disable internet access capabilities for devices that hold stored taxpayer data • Delete all information from all devices before disposing of them • Physically destroy all electronic storage media and paper documents before throwing away	• Spot data theft • Monitor EFIN/PTINs activity online • Recognize and guard against phishing scams and emails • Remain Safe on the internet	• Contact the IRS and law enforcement (FBI, Secret Service (if directed by IRS) and local police) • Contact states where you prepare state returns (email StateAlert@taxadmin.org) to find out info on who and how to report) and State Attorney General(s) • Contact experts, like security expert to investigate the root of the problem, and insurance company to determine loss

However, the writing of a security plan by itself does not end a tax practitioner's obligation to protect data. The U.S. Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, recognizes that the defenses to unauthorized intrusions does not end with the above items and therefore recommends that businesses ensure that it adopts and maintains the following ongoing protocols:

- Conduct anti-virus scans periodically across all systems with access to taxpayer data.
- Ensure anti-virus software remains up to date.
- Value encryption because it ''transforms data on the computer into unreadable files for the unauthorized person accessing the computer. Drive encryption may come as a stand-alone security software product. It may also include encryption for removable media, such as a thumb drive and its data.''[33]

A hallmark of an effective security plan includes the active participation of all employees. A modicum of vigilance should help to limit the amount of information potentially stolen by cybercriminals. The IRS offers a number of warning signs that a tax preparer has experienced a data theft.[34]

[33] IR-2018-150.

[34] IR-2018-152.

ISSN 0148-8295

- Returns filed on behalf of client rejected by the IRS because the IRS asserts that the taxpayer (same social security number) has filed a tax return already.
- A client, who has not filed return,
  - Receives unsolicited tax authentication letters, e.g. 5071C, 4883C and 5747C
  - Receives unexpected tax refunds.
- Clients receive unsolicited items from the IRS, such as,
  - Tax transcripts,
  - Notice about creation of unauthorized online account in taxpayer's name,
  - Notice about unauthorized access of online account or account disabled unexpectedly.
- Tax professionals discover
  - Number of returns filed per Electronic Filing Identification Number greater than total clients,
  - Network running slower than normal or locking out employees,
  - Computer cursors move or change without employee typing the keys,
  - Clients or other tax professionals responding to tax questions via email that they did not send.

In May 2002, the Federal Trade Commission (FTC) issued the final Safeguards Rule[35] mandating a security plan for service professionals, including tax professionals, that handle customer information that addresses the protection of client data under its statutory authority conferred under the Financial Services Modernization Act of 1999, more commonly known as Gramm-Leach Bliley (GLB) Act.[36] The Safeguards Rule became effective on May 23, 2003. Additionally, the FTC outlined via a checklist, appropriately named the Safeguards Rule Checklist (SRC), a number of steps that a business should take to protect client data. The SRC provides a number of practices that professionals should consider and implement that are divided into several broad categories, including employee management and training, information systems, and detecting and managing system failures.[37] The IRS has appended a number of suggestions to the Use the Safeguards Rule Checklist in IRS Pub. 4557 to incorporate how best to apply it to the business of tax practitioners. Tax practitioners offering services to individuals must therefore comply with the statutory requirements of the Safeguards Rule.

The IRS recently reminded tax practitioners that it views a violation of the Safeguards Rule as a violation of the relevant Authorized IRS e-file Provider rules, which may lead tax practitioners to suffer potential consequences, such as suspension from the e-file program. There is no recorded cases in which the IRS has in fact taken this action, based on such a violation of the rule, but the public statement that it has authority to take enforcement action for violation of a non-tax rule indicates a willingness to consider such censures.[38] Most tax practitioners would suffer a grievous fate economically should their participation in the e-file program be suspended.

MAINTENANCE AND EDUCATION PROGRAM

The creation of the security plan consistent with the Safeguards Rule does not by itself excuse future failures. In fact, a practitioner may devise a comprehensive security plan that incorporates many or all of the Security Six and other guidance recommendations, but the plan may grow stale due to lack of ongoing maintenance and education. Maintenance and education remain an important element of the security plan, and tax practitioners should perform regular maintenance activities to demonstrate vigilance and determine if any breach has occurred at the earliest possible time. The principal protocols found in such a maintenance program should include protecting and monitoring tax identification numbers, such as Electronic Filing Identification Numbers (EFINs), Preparer Tax Identification Numbers (PTINs), and Centralized Authorization File (CAF) numbers. The IRS outlined a number of protocols that constitute a reasonable maintenance program for the tax identification numbers regularly utilized by tax practitioners (see Table 4 below).[39] Performing the protocols will help protect the tax practitioner discover if cybercriminals have impersonated them by the use of the tax practitioner's IRS-issued identification numbers. Indeed, the IRS noted that cybercriminals post EFINs, PTINs, and CAF numbers (collectively the ''IRS-issued numbers'') on the Dark Web for use by other cybercriminals. The use of the IRS-issued numbers by cybercriminals provide legitimacy to fraudulently filed tax returns.

---

[35] 16 C.F.R. §314.

[36] See *generally*, Pub. L. No. 106-102, §501.

[37] IRS Pub. 4557, pp. 14-17.

[38] IR-2018-151; IRS Pub. 3415, p. 21.

[39] IR-2018-164, *Tax Security 101-IRS: Tax professionals must maintain, protect EFINs; Monitor EFINs, PTINs and CAF numbers* (Aug. 14, 2018).

ISSN 0148-8295

TABLE 4				
Guarding against misuse of IRS-issued numbers				
Questions	**Maintaining EFINs**	**Monitoring IRS-issued numbers**		
		EFINs	PTINs	CAFs
How often to perform?	Periodically (monthly)	Weekly	Weekly	Annually
What step to perform?	Review e-file application accuracy for any changes to people authorized, places, or telephone numbers	Generate online report to determine whether amount of returns filed matches your records	Generate online report to determine whether amount of returns filed matches your records	Identify outstanding authorizations that are for former clients and remove them

The IRS expects that tax practitioners will protect not only client data, but also defend their IRS-issued number(s) against unauthorized use by others, including by cybercriminals. The use of an IRS-issued number does not always indicate that the tax practitioner's client data has been compromised, but that does not excuse the tax practitioner from responsibility to act. The hallmarks of any misuse will reveal itself after completing these protocols.

Another key step to ensure that the tax practitioner achieves its security plan goals to safeguard client data requires ongoing employee education that reminds them of their role and responsibility to safeguard information. The education must reach all office employees and contractors because a single slip-up may compromise the confidentiality of the underlying information.[40] The best defense and the key to good security practices starts with ''an individual trained and alert to potential risks and threats.''[41] Tax practitioners should ensure that both they and all employees/contractors take all reasonable steps to safeguard client data. Where employees and contractors do not fulfill the security protocols outlined in the security plan, employees should be reminded as to the requirements and receive additional training to reinforce the importance of data security to the tax practice and its clients. Indeed, some businesses engage outside consulting firms to test whether their employees will fall victim to a cybersecurity ruse that might lead to future data compromise.

Intrusion Discovery and Disclosure Obligations

The adage that the slowest target in a group has the most to fear from a bear chasing the group seems appropriate to tax practitioners because of the varied sophistication in matters of cybersecurity. Therefore, implementing the above plan outlined by the Summit Partners should provide additional comfort and decrease cybersecurity risk when compared to other members that employ a less rigorous approach.

Nonetheless, even after the best efforts, a tax practitioner may suffer an intrusion and data may be compromised. In such instances, federal and state law controls who must disclose and when disclosure is required. The IRS wants tax practitioners to report data losses immediately to the IRS to help protect against IDTTF. The important parties a tax practitioner may need to notify concerning a data theft include:[42]

- Internal Revenue Service—local stakeholder liaison;
- Local police to file a police report;
- And, if directed by the IRS,
- Federal Bureau of Investigation (local office), and/or
- U.S. Secret Service (local office);
- Each state in which practitioner files state returns,
- Email the Federation of Tax Administrators at StateAlert@taxadmin.org to receive information on how to report to each state the victim information,
- State Attorney General for each state in which the tax practitioner prepares returns;
- Clients
- The Federal Trade Commission offers individualized templates on how and what to share with clients regarding the data theft via may contact the FTC at idt-brt@ftc.gov. A tax practitioner may need to send a letter to each victim to inform them of the breach, but should work with law enforcement on appropriate timing.
- Certain states may require the tax practitioner to offer monitoring /ID theft protection to victims of ID theft.
- The credit monitoring may be provided by contacting the various credit rating agencies, e.g., Equifax, Experian, and Trans Union.

[40] IR-2018-170, *Tax Security 101: Security Summit urges tax professionals to educate all employees about data security, computing safeguards* (Aug. 21, 2018).

[41] IR-2018-147.

[42] IRS Pub. 4557, which also references a Data Theft Information for Tax Professionals checklist.

ISSN 0148-8295

- If the IRS contacts the client that it has received two original returns with the client's social security number attached, then the client should complete IRS Form 14039, Identity Theft Affidavit and return it to the IRS.

The persons and groups to contact may be daunting, but the FTC offers several self-help guides that address the process of responding and recovering from the data loss events.[43] These self-help guides should aid in crafting the response to the data breach and limit the damage while informing clients and other interested parties about the relevant resources available to halt further damage to clients.

The IRS has outlined five actions that all tax practitioners should take to achieve better outcomes that bear repeating and emphasis:

1. Recognize the different fraudulent schemes
2. Create a data security plan
3. Review internal control of their business
4. Report data thefts
5. Remain connected with IRS[44]

FINAL THOUGHTS

The IRS continues to remind tax practitioners about the prevalence of attacks in a recent announcement that hundreds of tax professionals suffered a client data breach.[45] The affected tax professionals offered four lessons learned to help avoid the devastating data loss to the clients and their own business.

- Secure cyber insurance coverage for the costs incurred directly resulting from the data theft, including technical experts to remedy the deficiency and inform the victims.
- Adopt protocol to password protect each client account separately in tax software and on the computer system or network. While clearly more work to maintain, many tax software products allow such functionality and provide a critical safeguard against the threat cybercriminals pose.
- Use a virtual private network (VPN) for remote connections, which allows teleworkers to connect in a secure manner to the practitioner's computer system and transmit and receive information. If there is no VPN, the use of remote access software might allow cybercriminals to remotely access and hijack client accounts via the tax practitioner's computer and e-file returns, and have the refunds diverted to the cybercriminal's own bank accounts.
- Keep all security software updated, including operating systems, anti-malware, anti-virus software, etc. It is a good practice for tax practitioners to select their security software to update automatically versus manually. New threats emerge on an almost daily-basis, so the security software should update in real-time to defend against the near constant scheme barrage.

In the case of a bank that receives a visit from a person like Willie Sutton today, while it could be emotionally traumatic it might not hold long-lasting financial consequences when compared to an intrusion by a cybercriminal of a tax practitioner's client records. Just like most banks maintain an insurance bond against robbery that offers a reliable financial safety net to the offended banks, tax practitioners may hold an insurance policy that covers cybersecurity losses, including client loss within limits. However, a tax practitioner that suffers the loss of client data faces a seemingly longer-lasting threat to their continuing business, i.e., loss of prestige and potential client exodus without any prospect of return. These consequences may occur naturally upon mandated disclosure, then government authorities may impose additional measures, e.g., denial to participate in the e-file program, should they deem the tax practitioner's data security posture lax or the intrusion response ineffective. In any event, a tax practitioner's inattention to cybersecurity risk may lead to catastrophic consequences, and as such, a tax practitioner's defense of the integrity of the tax system may be the only acceptable path to lessen the risk of potential banishment due to the will of either or both the IRS and/or affected clients.

---

[43] See for more detail, FTC, Data Breach Response: A Guide for Business.

[44] IRS Pub. 4557.

[45] IR-2018-161, *Tax Security 101-Tax professionals victimized by data thefts offer hard-won security lessons to colleagues* (Aug. 7, 2018).

ISSN 0148-8295