Chapter 5. Protecting You and Your Clients from Fraud

Tax professionals continue to be a prime target for cybercriminals. We must all take responsibility for protecting client data from theft.

To provide you guidance on data security, the IRS joined with state agencies and the tax industry to form the Security Summit. The Security Summit has created awareness campaigns such as:

- Protect Your Clients; Protect Yourself — Summer 2022
- Boost Security Immunity: Fight Against Identity Theft
- Protect Your Clients; Protect Yourself: Tax Security 101
- Tax Security 2.0
- Working Virtually: Protecting Tax Data at Home and at Work

This year's theme, Protect Your Clients; Protect Yourself — Summer 2023, is focused on raising awareness among tax professionals about the importance of maintaining strong security. This can help protect sensitive taxpayer data that tax professionals have while also protecting their business from identity thieves.

The IRS, state tax agencies, and the nation's tax industry continue to see a steady stream of attacks aimed at the nation's tax professional community to steal sensitive tax and financial information from clients. As part of this campaign, partners of the Security Summit encourage tax professionals to use its security plan template (Written Information Security Plan) designed to help tax professionals create and implement a data security plan.

Secure Your Systems

Title V, Subtitle A of the Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act, and the Safeguards Rule (Code of Federal Regulations, Title 16, Chapter I, Subchapter C, Part 314) require certain entities - including tax return preparers - to create and maintain a security plan for protecting client data.

According to the Federal Trade Commission (FTC), each company, as part of its plan, must:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate how effectively current safeguards control these risks.
- Design and implement a safeguards program with regular monitoring and testing.
- Select service providers who maintain appropriate safeguards. Ensure the contract requires the provider to maintain safeguards and oversee their handling of customer information.
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations or results from security testing and monitoring.

Note that the FTC is re-evaluating the Safeguards Rule and has proposed new regulations. Watch for any changes in the Safeguards Rule and their effect on the tax preparation community.

These publications will help you get started:

- IRS Publication 4557 outlines your obligations to protect client information. It also has a checklist for creating and maintaining a security plan for your digital network and office.
- FTC Cybersecurity for Small Business includes practical tips on creating and implementing a plan for safeguarding personal information.
- NIST's Small Business Information Security – The Fundamentals (NISTIR 7621, Revision 1) provides an overview of five principles to secure data: identify, protect, detect, respond, and recover.
- IRS Publication 5293 provides basic steps you and your firm can take to protect client data. This step-by-step guide makes data security achievable for tax professionals and firms of all sizes.

Spot Data Theft

You or your firm may be a victim of data theft and not even know it. Here are some common signs of data theft:

- Your clients' e-filed tax returns begin to be rejected because returns with their Social Security Numbers were already filed
- The returns filed for a taxable year with your firm's Electronic Filing Identification Number (EFIN) exceed your number of clients
- Tax professionals or clients respond to emails you or your firm did not send
- Your network computers slow down
- Computer cursors move or numbers change without your input
- Network computers lock you out
- Your clients receive:
  - IRS authentication letters (5071C, 4883C, or 5747C) for returns they did not file
  - Refunds for returns they did not file
  - Tax transcripts they did not request
  - IRS online services account emails stating an account was created when they did not create one
  - IRS online services account emails stating their account was accessed or disabled when they did not request it

Create a Data Theft Response Plan

If you fall victim to data theft, immediately:

- **Report it to the** local IRS stakeholder liaison. Stakeholder liaisons will notify IRS Criminal Investigation and others within the agency. The IRS can block fraudulent returns in your clients' names and assist through the process. If the data theft involved an IRS impersonation scam, you should also report it to the Treasury Inspector General for Tax Administration.
- **Email the Federation of Tax Administrators at** StateAlert@taxadmin.org. Get information on how to report victim information to the states. Most states require that the state attorney general be notified of data breaches. The notification process may involve multiple offices.
- **Call the Minnesota Department of Revenue** at 651-296-3781 or 1-800-652-9094. We will connect you with a fraud coordinator who can assist with determining whether you are a victim and which clients' or

tax professionals' information was accessed. We can take steps to block fraudulent returns in your clients' names.

- **Submit an identity theft affidavit for businesses and other entities**. Federal Form 14039-B makes it easier for businesses, estates, trusts, and tax-exempt organizations to report identity theft to the IRS. Submitting this form will quickly let the IRS help entities who are victims of identity theft. To access the form, see Report Identify Theft for a Business on the IRS website.

Find Data Theft Information for Tax Professionals on the IRS website.

Stay Vigilant

Stay ahead of the thieves by taking certain actions daily or weekly to ensure your clients and your business remain safe:

- **Track your daily e-file acknowledgements.** If there are more acknowledgements than returns you know you filed, dig deeper.
- **Track your weekly Electronic Filing Identification Number (EFIN) usage.** The IRS posts the number of returns filed with your EFIN weekly.
    - Access your IRS e-Services account and your EFIN application.
    - Select "EFIN Status" from the application.
    - Contact the IRS e-Help Desk if your return totals exceed your number of returns filed.
    - Keep your EFIN application up to date with all phone, address, or personnel changes.
- **Track your weekly Preparer Tax Identification Number (PTIN) usage.** If you file 50 or more returns as an attorney, Certified Public Accountant (CPA), enrolled agent (EA), or Annual Filing Season Program participant, you can check your PTIN account for a weekly report:
    - Access your online PTIN account.
    - Select "View Returns Filed Per PTIN."
    - Complete federal Form 14157 to report excessive use or misuse of your PTIN.
- **If you have a Centralized Authorization File (CAF) Number,** keep your authorizations up to date. Use a Freedom of Information Act (FOIA) request to secure your CAF 77 client listing. Review the list to ensure it is accurate. Remove authorizations for clients you no longer work with and for any taxpayers who have never been your clients (a possible ID theft indicator). For more information, see IRS Publication 947.
- **Create your IRS online accounts using the multi-factor Secure Access authentication** to help prevent account takeovers. For details, see the IRS's Secure Access page.

Recognize Phishing Scams

Cybercriminals commonly steal data through phishing scams. Phishing often occurs through unsolicited emails or websites luring unsuspecting victims to provide personal information.

The thief may pose as your tax software provider, your data storage provider, your bank, the IRS, or even a prospective client. Thieves may even pose as colleagues whose email accounts were compromised. For tips on defending yourself from phishing scams, see Report Phishing and Online Scams from the IRS.

Educate all employees in your office on the dangers of phishing scams. These scams can result in cybercriminals taking over your computer or accounts to steal client data.

- Thieves may hijack your email account to send spam emails under your name, tricking your colleagues and clients into disclosing information.
- An even more successful tactic is spear-phishing, where a thief specifically targets you or your firm, perhaps from seeing your email address online.
- Generally, phishing or spear-phishing emails have an urgent subject line such as "Update Your Account Now," enticing you to open a link or attachment.
    - **Link:** The link may take you to a fake webpage designed to look like a familiar website such as IRS e-Services. There may also be a call to action, such as "Click Here Now." You may be asked to enter your username and password for an account, but you are actually disclosing your credentials to thieves.
    - **Attachment:** Attachments may contain software that can infect your computer and network systems (malware). A common malware is keystroke tracking, which allows the criminal to see the words you type on your device, including your username and password to various accounts. This malware gives them access to your tax software, bank, or encrypted client files.
- A legitimate business should never request personal or sensitive information be sent to them via email, unless it's through a secured mail service.

Guard Against Phishing, Spear-phishing, and Whaling Emails

Educated employees are the key to avoiding phishing and related scams, but these simple steps can also help protect you:

- Use separate personal and business email accounts protected with strong passwords and multi-factor authentication.
- Install an anti-phishing toolbar, which may be included in security software products, to help identify known phishing sites.
- Use security software to help protect systems from malware and scan emails for viruses.
- Never open or download attachments from unknown senders, including potential clients. Try calling them first to confirm they sent you something.
- If you must email files with clients, send only encrypted and password-protected documents.
- Do not respond to suspicious or unknown emails. If suspicious emails are IRS-related, forward them to phishing@irs.gov.

Be Safe on the Internet

Data security requires ongoing awareness about the threats posed from a variety of sources, including browsing the internet. Here are some general steps for staying safe online.

- Keep your web browser software up to date so it has the latest security features.
- Scan files using your security software before downloading them.
- Delete web browser cache, temporary internet files, cookies, and browsing history regularly.
- When possible, only use web addresses that start with "HTTPS" (https://www.irs.gov).

- Avoid accessing business emails or information from public Wi-Fi connections.
- Disable stored password features offered by some operating systems.
- Enable your browser's pop-up blocker, and do not call numbers listed on pop-ups.
- Do not download files, software, or applications from unknown websites.
- Note instances where your browser's home page changes. This could be a sign of malware or intrusion.
- Use a Virtual Private Network (VPN) - a secure, encrypted network to transmit data between a remote user and the company.

Stay Connected

We alert tax professionals as quickly as possible when we learn of new scams, which are especially common during the filing season. Subscribe to our Tax Scam and Fraud Alerts email lists so you can stay informed of the latest alerts and tax administration issues.

Encourage clients to obtain Identity Protection PINs (IP PINs)

The IP PIN Opt-In Program can protect clients from tax-related identity theft and is available to anyone who can verify their identity. While the program is free, we need your help letting clients know about it. For details, see Get An Identity Protection PIN on the IRS website or IRS Publication 5367.

For security reasons, you cannot obtain an IP PIN on behalf of clients. They must obtain their own IP PIN.

State Forms to Help Report ID Theft

These forms help manage the reporting of identity theft to Revenue and allow your clients to request copies of fraudulently-filed returns.

If your client believes they are a victim of identity theft, they should call us at 651-296-3781 or 1-800-652-9094. Then, they should complete and submit Form M1ID, Identity Theft Affidavit. This will alert us to the issue and help us detect any potential fraud on their account. We will notify your client if a fraudulent return was filed or not.

If your client receives a letter informing them a Minnesota return was fraudulently filed under their name, they can contact us for a copy of the return.

- If your client wants a copy of the fraudulent return for their records, they should complete Form REV189, Request for Copy of Return Related to Identity Theft.
- If your client wants to send a copy of the fraudulent return to a specific law enforcement agency, they should complete Form REV190, Authorization to Release Return Related to Identity Theft.