No-Nonsense Guide for Firm Owners

By now, most tax preparers are aware they need to comply with the FTC Safeguards Rule and IRS Publication 4557. Failure to do so could result in stiff penalties.

Chris Farrell • Jun. 28, 2023

By Chris Farrell, CPA.

By now, most tax preparers are aware they need to comply with the FTC Safeguards Rule and IRS Publication 4557. Failure to do so could result in stiff penalties, yet many firms have not been able to make this a priority.

And what if you don't provide tax? The first step is to figure out if you are subject to

It isn't difficult to have more than 5K consumers (targets) in firm data banks, stored files, and software, meaning that even the smallest firms may need to comply with the FTC Safeguards Rule.

The best place for tax pros and non-tax firms to begin their compliance journey is by creating and rolling out a Written Information Security Plan (WISP). This is required under Publication 4557 and is just good business practice for any firm who handles sensitive client information.

Publication 4557 is broken up into four parts with 12 steps, and all of them need to be addressed in the WISP. The steps are listed below. Use the list as a checklist to see what still needs to be acted upon in your firm.

1. **Take basic security steps**
    - Recognize phishing emails
    - **Create a written information security plan (WISP)**
    - Review internal controls
        - Anti-malware, strong passwords, backup, final review of return direct deposit information, wipe old computer drives, limit access to data, check EFINs and PTINs, withdraw Power of Attorney
    - Report data loss to IRS Stakeholder liaison
    - Connect to IRS for updates
    - Educate clients on PII and risks
    - Review FTC security tips
2. **Use security software**
    - Anti-virus/anti-malware
    - Use both signature-based and heuristic-based applications
    - Anti-spyware to prevent unauthorized applications from harvesting data
        - On each device, or, applied through the network
    - Firewalls to block unwanted connections

- Drive encryption

- Ensure WPA2 encryption
- Reduce transmission power to the lowest possible setting
- Change network name to something that does not identify the nature of your business
- Do not use public networks to access sensitive information without a VPN

5. **Protect stored client data**
   - Encrypt all disk drives
   - Backup data daily or continuously, using multiple forms of media
   - Avoid using USB drives, particularly if they contain client data and you are using them on devices you do not control
   - Avoid installing unnecessary software
   - Maintain an inventory of all devices on which client data is stored and control internet access on these devices
   - Securely delete all data before disposing of a device
6. **Spot data theft**
   - Any of the following may indicate data theft or on-going data theft
     - Client tax returns are rejected because a return was already filed
     - Clients receive transcripts they did not request
     - Number of returns filed with the firm's EFIN exceeds the firm's number of clients
     - Computers are running more slowly than normal
     - Cursors moving or changing on their own
     - Computers locking out practitioners
7. **Monitor EFIN/PTINs**
   - Monitor the number of returns filed using EFINs and PTINs
   - Ensure your Centralized Authorization File (CAF) number is up to date and withdraw any authorizations for those who are no longer clients
8. **Recognize phishing scams**
   - You don't know the sender

- Contains a link or an attachment

- Educate all staff members including partners and executives.

0. **Be safe on the internet**
    - Keep browsers up-to-date
    - Scan files for malware before downloading them
    - Delete browser cache, temp internet files, cookies, and browser history periodically
    - Always connect to secure sites: (https://) instead of (http://)
    - Do not access sensitive information, including business emails, from unencrypted public Wi-Fi
    - Don't store passwords
    - Enable pop-up blockers
    - Don't download data or publications from unknown sites
    - Note if your Home page changes
    - Report data loss to IRS and State authorities
11. **Report client data theft to your local IRS stakeholder liaison**
    - If directed by the IRS, contact the FBI and Secret Service
    - Contact local police to report the data breach
    - Notify state departments of revenue for which you prepare state returns
    - Many state breach notification laws require reporting to the Attorney General of the state
12. **Respond and recover from a data loss**
    - Update your local IRS Stakeholder Liaison because the IRS cannot accept third-party reports of identity theft
    - Review the FTC's Data Breach Response: A Guide for Business
    - Determine how the breach occurred and fix the problem before you resume processing (with a new EFIN)
    - Develop or update your firm's data security and continuity plan
    - Create full, encrypted backups of all files
    - Consult with your insurance company regarding potential reimbursements

Refer to the article ***Rolling out Your Firm's WISP – A Practical Guide for Firm***

2. That qualified individual creates a written risk assessment, then designs regular tests and controls to keep your data and network safe. They also have to report to your Board of Directors about this regularly.

3. Ensure that all vendors are using good security practices.

4. Train staff on the FTC's broad definition of sensitive data – it even includes your clients' list of customers.

Another way to fast track compliance is to take a training course designed to walk you through the steps and ensure you have the resources you need to quickly create your WISP and roll it out. The Grove is a great place to start – Randy Johnston, CPA, Dawn Brolin, CPE, CFE, Steve Perkins, CIO of HoganTaylor LLP, along with Andrew Lassise from Tech4Accountants have collaborated on a course designed to help firm leaders fast-track their compliance with both IRS Publication 4557 and The FTC Safeguards Rule.

=======

Chris Farrell, CPA is cofounder of Liscio, Inc. and serves as its Chief Executive Officer. Chris has more than 25 years of experience in the accounting, finance and software industries. Prior to Liscio, he co-founded and led SpringAhead and Tallie where he served as Chief Executive Officer. He also served as the Chief Financial Officer of Occam Networks, the Corporate Controller of C-Cube Microsystems and as an auditor for Arthur Andersen. He holds a Masters degree in Business Administration from UCLA's Anderson School of Management and received his CPA license in California.

Advisory • Firm Management • Security • Taxes