K2's Safeguarding Taxpayer Data

A Guide For Your Required Security Plan

Learning Objectives

Upon completing this session, you should be able to:

- List examples of basic security steps and how to implement them
- Identify the signs of data theft and how to report data theft
- List examples of how to respond and recover from a data loss
- Identify examples of specific compliance issues found in the FTC Safeguards Rule

Today's Agenda

- Data security requirements
- Risks associated with non-compliance
- Security tools and processes that should be used

WHAT SECURITY REQUIREMENTS ARE IMPOSED BY THE IRS AND THE FTC?

Protecting Client Information

Data thefts at the offices of tax professionals are on the rise

Data security is necessary for every tax professional,
whether a partner in a large firm or a sole practitioner

All staff members have a role in protecting sensitive taxpayer information

Protecting taxpayer data is good business

Protecting taxpayer data is the law

Data Thefts Are Rising

- Consider the breadth of sensitive information on file in firms that prepare taxes
  - Names
  - Dates of birth
  - Social Security numbers
  - Bank account and routing numbers
  - Credit card statements
- Accountants and tax preparers provide a "target-rich" environment

Data Security Is Necessary

- Every staff member must be *educated* about the risk associated with handling sensitive information
- *Training* and *reinforcement* are the most important steps we can take to mitigate the risks to our firms and to our clients

All Staff Members Have A Role

- All staff members have a role and must be involved in security, from the Managing Partner to the newest intern
- A tax professional may send PDFs of tax returns as unencrypted email attachments
- Custodial staff may not shred paper waste containing taxpayer data before disposal
- From top to bottom, everyone must know and execute their information security responsibilities

Protecting Data Is Good Business

How much would a data breach cost your firm?

How many clients would you lose?

What would you pay in legal costs? Are they covered by insurance?

Protecting Data Is The Law

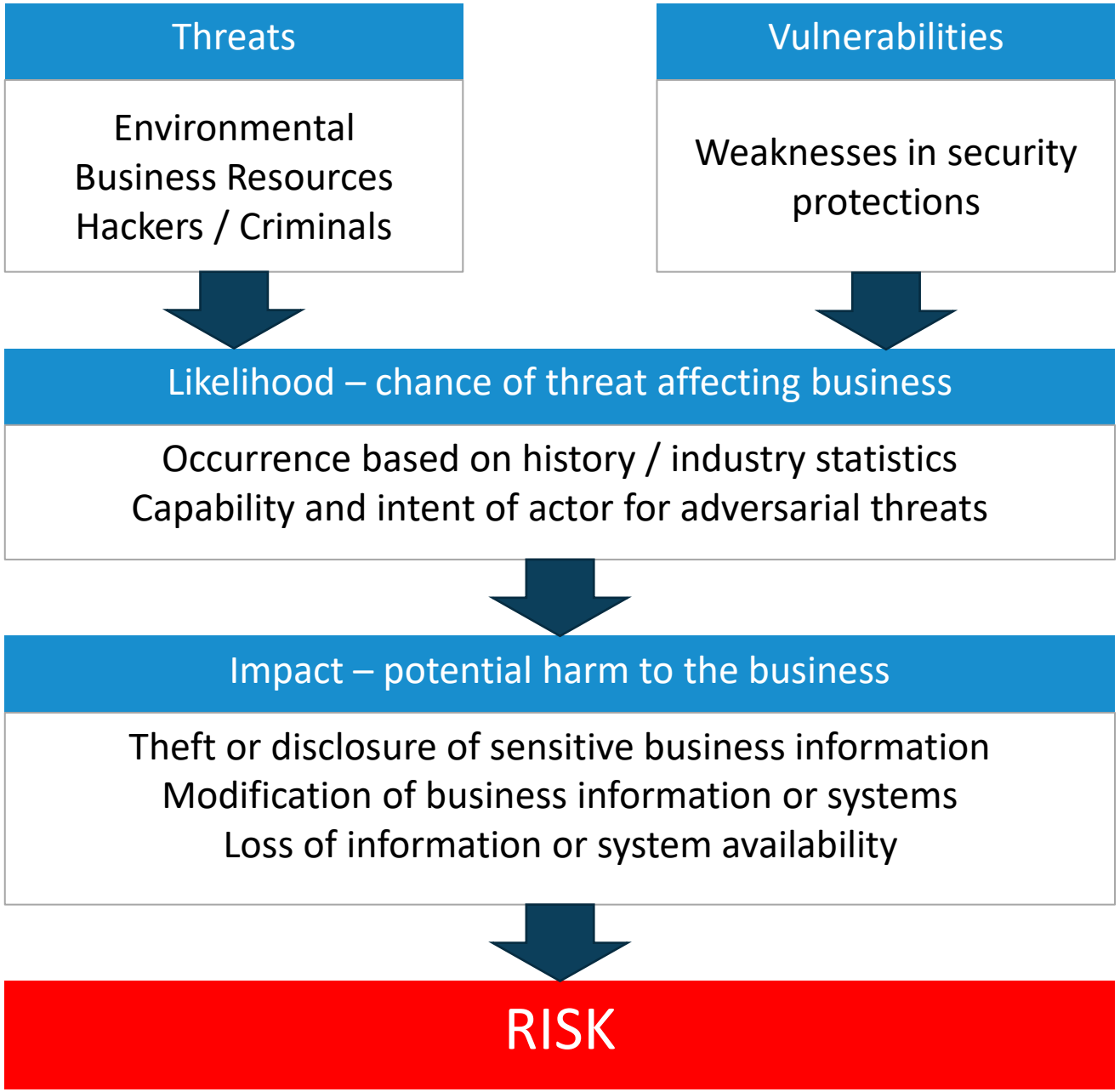
- The Federal Trade Commission (FTC) has jurisdiction to set data safeguarding regulations for various entities, including *tax return preparers*
- Known as the *Safeguards Rule*, the FTC requires organizations to have measures in place to keep customer information secure
  - Companies subject to the rule are responsible for taking steps to ensure that their affiliates and service providers safeguard client or customer information in their care
- Firms could be subject to other laws and regulations at the state or local level, such as data encryption laws or security breach notification laws

Protecting Taxpayer Data Is The Law

Additionally, *online providers* must follow the six security and privacy standards in IRS Publication 1345

1) Extended validation SSL certificate
2) External vulnerability scan on a weekly basis
3) Information privacy and safeguard policies, certified by a third-party
4) Protection against bulk filing of fraudulent income tax returns
5) Public domain name registration
6) Reporting of security incidents, as soon as possible, but not later than the next business day

WHAT ARE THE RISKS ASSOCIATED WITH NON-COMPLIANCE?



What Is Risk?

Many Types Of Risk

- Damage to information or information systems
- Regulatory fines and penalties / legal fees
- Decreased productivity
- Loss of information critical to running your business
- An adverse reputation or loss of trust from customers
- Damage to your credit and inability to get loans from banks
- Loss of business income

FTC Safeguards Rule Penalties

- The FTC deems tax preparers "financial institutions" under the Gramm-Leach-Bliley Act
- Compliance with the Act is mandatory
- Non-compliance can lead to fines of up to $100,000 or imprisonment for each violation
- Officers and directors can be fined up to $10,000 for each violation

TOOLS, PROCESSES, AND PROCEDURES TO MINIMIZE RISK?

IRS Publication 4557

1) Take basic security steps
2) Use security software
3) Create strong passwords
4) Secure wireless networks
5) Protect stored client data
6) Spot data theft
7) Monitor EFIN/PTIN
8) Recognize phishing scams
9) Guard against phishing emails
10) Be safe on the internet
11) Report data loss to IRS and State authorities
12) Respond and recover from a data loss

TAKE BASIC SECURITY STEPS

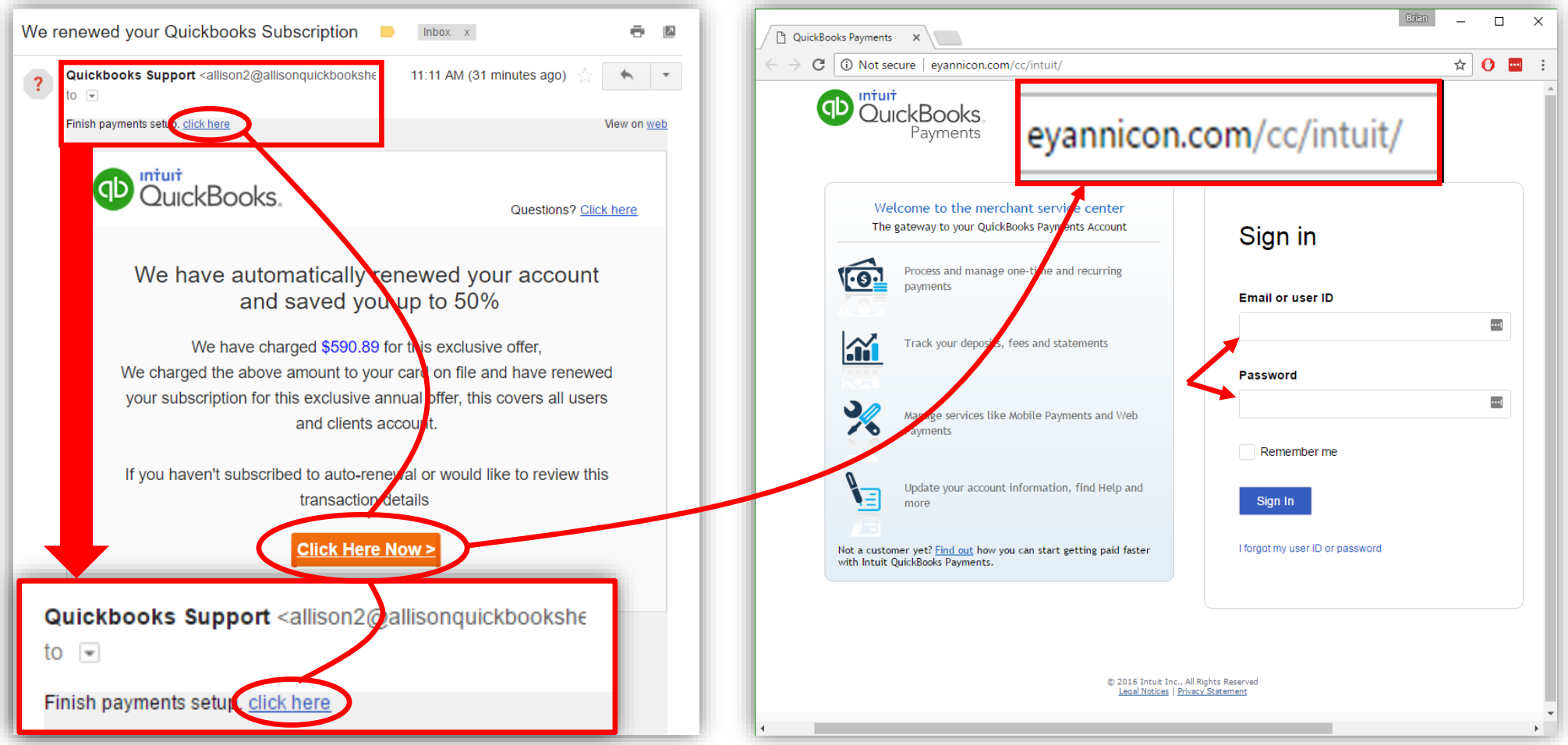
Risk Of Phishing Emails

- Phishing email threats are exploding!
- 91% of all data breaches start with a phishing attack, according to KnowBe4 (www.knowbe4.com)
- Phishing coupled with social-engineering creates a very risky situation
- The fundamental rule remains, if you don't know the person who sent it to you or you weren't expecting it, don't open it or click on it

Recognize Phishing Emails

- You don't know the sender
- Contains a link or an attachment
- Uses poor spelling, poor grammar, or both
- The domain is VERY SIMILAR to your firm or company's domain
- The domain is a "personal grade" domain, such as gmail.com
- Includes low-resolution graphics
- The message communicates a false sense of urgency

Phishing Attack Posing As Intuit



Actual phishing message received by K2 Associate

Consider Just How Much Damage A Successful Phishing Attack Could Cause An Accounting Firm

Here's One Example

CALIFORNIA CPA FIRM HACKED

Accounting Today

August 25, 2017

accountingTODAY All Sections

NOW READING: The Latest | California CPA firm reports data breach | IRS sees new filing season scam hitting tax pros | Weaver acquires Condon tax practice | Voices Tax season

California CPA firm reports data breach

By
Michael Cohn

Published
August 25 2017, 2:58pm EDT

More in
Data breaches
Identity theft
Identity theft protection
Tax practice

Print Reprint

[redacted] a CPA firm based in [redacted], Calif., has disclosed it detected unauthorized access to its computer systems from abroad while filing tax returns.

The firm said in a news release Thursday that it experienced "unusual activity" while filing two tax returns on extension. It said it immediately notified the Internal Revenue Service, had its local IT firm review the system and hired a specialized forensic IT firm to investigate. On July 10, the forensic IT firm found there was unauthorized access to the firm's system from a foreign IP address on June 14, 2017.

California CPA Firm Hacked

- Firm experienced "unusual activity" while filing two tax returns on extension
- Hired specialized forensic IT firm to investigate
  - There was unauthorized access to the firm's network from a foreign IP address on June 14, 2017
  - The hackers may have accessed information provided to the tax authorities, such as name, date of birth, phone number, address, Social Security number, W-2 and 1099 information, driver's license details, and bank accounts
  - The firm said some of its own partners' and employees' information may also have been exposed

California CPA Firm Hacked

- Firm recommended that clients and others affected should
  - Change their bank account numbers provided to the firm
  - Set up 90-day fraud alerts with Equifax, Experian, and TransUnion
  - Consider placing a credit freeze on their accounts
  - File a complaint with the FTC and local law enforcement if they become a victim of identity theft

Warnings to Practitioners

- Thomson Reuters posted a security alert in late June 2017 warning accounting firms of a fraudulent e-mail requesting validation of their login credentials to "add new security measures"
- Also from the blog post:
  - It's designed to look like a valid e-mail from your tax and accounting software provider
  - Just another example of bad actors using social engineering tactics to trick staff into clicking fraudulent links and providing login credentials to access sensitive client and firm data.

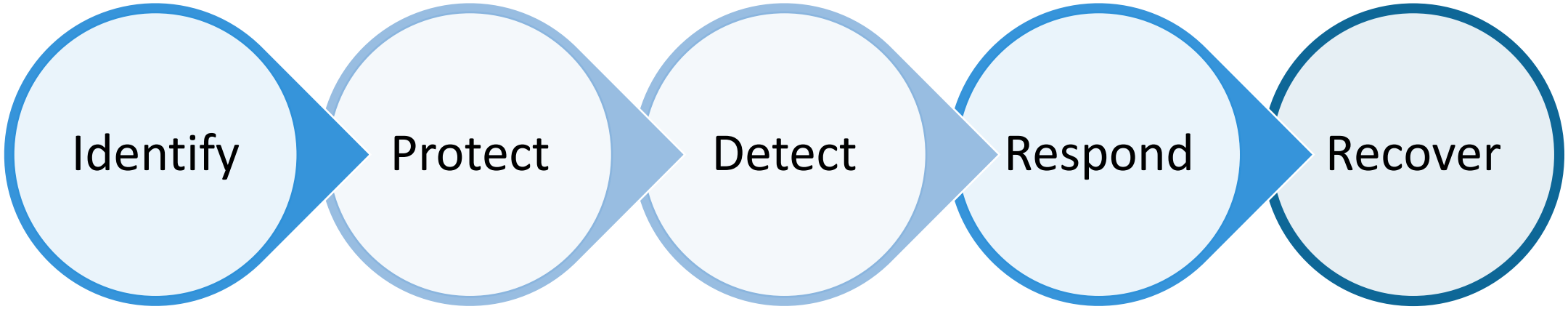
What To Do About Phishing?

- Train your staff, train your staff, train your staff!
- Consider blocking or quarantining messages that contain attachments
- Implement secure email gateways such as Barracuda
- Utilize post-delivery protection platforms such as Ironscales
- If your email is provided through a Microsoft 365 or Office 365 subscription, take advantage of tools available from Microsoft
  - Anti-phishing policies in Microsoft Defender for Office 365
  - Campaign views
  - Attack Simulator in Microsoft Defender for Office 365

Create A Data Security Plan

- NIST provides a five-pronged framework for its recommended data security plan
- The plan is outlined in NIST.IR Publication 7621
- "Small Business Information Security: The Fundamentals," *National Institute of Standards and Technology*

NIST's Security Framework



Identify Resources And Risks

Identify and control who has access to your business info

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for info security

Protect Or Limit Exposure Of Data

- Limit employee access to data and information
- Install surge protectors and uninterruptible power supplies
- Patch your operating systems and applications
- Install and activate software and hardware firewalls on all networks
- Secure your wireless access points and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old devices and media safely
- Train your team members

Employ Controls To Detect Issues

- Install and ensure continual updates of anti-malware tools
  - Carefully consider whether signature-based tools, heuristic-based tools, or both would be best for your firm
- Maintain and monitor access logs
  - Use logs to detect *who*, did *what*, and *when* did they do it, assuming log-in credentials are not compromised
- Consider Data Loss Prevention tools for email and file storage

Develop A Plan To Respond

- Develop a comprehensive and continually update a plan for disasters, including information security incidents
  - Don't focus so much on the cause of the event (fire, flood, data security breach) as the impact of the event (we can't access our data)
- The plan should include:
  - Staff roles and responsibilities to execute the plan
  - What should be done with IT systems in case of an incident
  - Who to call and when (law enforcement, insurance provider, state or federal agencies required by breach notification laws)
  - What types of events warrant executing the plan (a five-minute web site glitch or a ransomware attack)

Be Able To Recover Systems

- Full backups of all important information, at least monthly, with effective post-backup testing
- Incremental backups of data, at least weekly, but preferably in real-time given the availability of reliable cloud-based solutions
- Consider the need for cyber insurance policies, including those covering any outside IT consultants or support staff
- Re-assess your plan periodically to determine if it remains valid and up-to-date, given changes to your firm environment

NIST Recommendations

- Pay attention to the people you work with (including clients)
- Be careful of email attachments and web links
- Use separate personal and business computers and other devices
- Do not connect personal or untrusted storage devices to your corporate devices
- Be careful what you download, including software
- Do not share personal or business information
- Watch for harmful pop-ups
- Use "long-and-strong" passwords and multi-factor authentication
- Conduct on-line business securely

Review Data Security Controls

1) Do we have anti-malware tools on all devices? Are the definitions updated automatically?
2) Are we using strong passwords? Password management tools? Multi-factor authentication?
3) Is all data encrypted while stored? Are all network connections encrypted? Do staff members use VPN's when connecting while away from the office?
4) Are backups done at least daily and stored on devices NOT connected to the server or network?

Review Data Security Controls

5) Do we make a final review of return information, particularly direct deposit information, before e-filing?
6) Do we wipe clean all drives, computers, phones, printers, scanners, copies, and other devices before disposing of them?
7) Have we effectively limited access to data within the firm to those who have a "need to know?" (Should a newly-hired auditor fresh out of college need access to the 1040 files of our highest-earning clients?)
8) Do we check our IRS e-Services account weekly for the number of returns filed with EFINs and PTINs?

Monitor EFINs And PTINs

- For EFIN totals
  - Access your e-Services account and your EFIN application
  - Select **EFIN Status** from the application
  - Contact the IRS e-help Desk if the return totals exceed the number of returns you filed
- For PTIN totals
  - Access your online PTIN account
  - Select **View Returns Filed Per PTIN**
  - Complete **Form 14157, Complaint: Tax Return Preparer**, to report excessive use or misuse of a PTIN

Report Data Theft/Loss To The IRS

- 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

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

Create Strong Passwords

- At least 12 characters, including upper and lower-case letters, numbers, and special characters
- Separate password for every application or service
- Never re-use old passwords
- Use password management tools to ease the burden
  - McAfee Anti-Virus Plus
  - Bitdefender Anti-Virus Plus
  - Webroot SecureAnywhere
  - LastPass Anti-Virus Premium

Secure Wireless Networks

- Change default passwords on all routers
- Ensure WPA3 encryption
- Reduce transmission power to the lowest possible setting that provides adequate coverage
- Change the name of your network to something that does not identify the nature of your business
- Do not use public networks to access sensitive information without the protection of a VPN

Protect Stored Client Data

- Encrypt all disk drives – Windows **BitLocker** is a good tool for this
- 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

Spot Data Theft

- Any of the following may indicate data theft or on-going data theft
  - Client tax returns are rejected because a return using the SSN was already filed
  - Clients receive transcripts they did not request
  - Number of returns filed with your firm's EFIN exceeds the firm's number of clients
  - Computers are running more slowly than normal
  - Cursors moving or changing without someone using the keyboard or mouse
  - Computers locking out practitioners

Monitor EFINs And PTINs

- Monitor the number of returns filed using EFINs and PTINs
- If the EFIN volume appears excessive, contact the IRS e-Help Desk
- If the PTIN volume appears excessive, complete **Form 14157, Complaint: Tax Return Preparer**
- Ensure your **Centralized Authorization File** (**CAF**) number is up to date and withdraw any authorizations for those who are no longer clients

Guard Against Phishing Attacks

- Phishing represents a tremendous risk to all businesses today, including tax preparers
- Be especially aware of emails that contain unsolicited links or attachments, particularly if they come from unknown parties
- Most importantly, educate all staff members including partners and executives!

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

Recover From A Data Loss

- Update your local IRS Stakeholder Liaison because the IRS cannot accept third-party reports of identify theft
- Review the FTC's *Data Breach Response: A Guide for Business* available as a PDF online
- 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

FTC Safeguards Rule Compliance

- The Gramm-Leach-Bliley Act (GLB) requires companies designated as financial institutions to comply with certain requirements and *professional tax preparers are included in the definition of financial institutions*
- Tax preparers are subject to the GLB Safeguards Rule
- Non-compliance can lead to steep fines or imprisonment

Safeguards Rule Requirements

- *Firms must create a security plan* that is appropriate for the organization's size and complexity
  - A plan for a sole proprietor will be markedly different than the one for a Big Four firm
- A firm's plan must be appropriate *for the nature and scope of the services offered and the sensitivity of the customer information* handled by the firm

Specific Requirements Of The Rule

- Designate one or more employees to coordinate the plan
- Identify and assess risks to customer information in each relevant area of the firm's operations and evaluate the effectiveness of the current safeguards for controlling these risks
- Design and implement a safeguards program and regularly monitor and test it

Specific Requirements Of The Rule

- Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information
- Evaluate and adjust the plan considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring

How Does The Work-From-Home (WFH) Environment Change Things?

Take Aways

- Every firm, regardless of size, is at risk!
- Consider the volume of private and sensitive information that tax practitioners store and how much criminals would like to get their hands on this information
- Firms are bound by the *FTC Safeguards Rule* to protect client data and failure to do so could lead to criminal sanctions
- Common sense goes a long way toward addressing security issues, so follow the guidelines and checklists to reduce your firm's risk to a reasonable level

Authoritative Resources

- **IRS Publication 1345**, "*Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*"
- **IRS Publication 4557**, "*Safeguarding Taxpayer Data*"
- **IRS Publication 5293**, "*Protect Your Clients; Protect Yourself*"
- National Institute of Standards and Technology, "***Small Business Information Security: The Fundamentals***"

E-mail:

randy@k2e.com

brian@k2e.com

QUESTIONS?