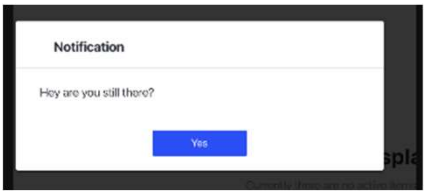
Protecting Tax Information—Cyber-Security for the Tax Professional

(PTIC4)

KAPLAN

Tips for a Successful Experience

- **Technical Difficulty?** Try refreshing your page, reconnecting to the class, or rebooting (chat the moderator if you do this, so they can keep track of your presence). Also, logging in under your company's VPN may cause technical difficulty. Turn off your pop up blocker! Tech Support Team 866.265.1561 Option 1 then Option 2
- **Earning CPE:** Throughout the presentation a presence manager will pop up to check your attendance. Click on the "Yes" box to record your attendance. Credit is earned by acknowledging 75% of these pop-ups per hour. The pop ups are random per participant.



- **Once you are logged in please do not log out even during breaks.**
- **Materials:** All materials for today's presentation are available in the lower left side of the webcast screen in the box directly under the Chat box. Click on them to download.
- **Questions:** Use the Chat box in the lower left side of the webcast screen to ask any questions you may have about today's webcast. Someone is available to assist with your technology related concerns. The instructor will address your content related questions during the presentation or follow up after.

Program Objectives

- List risks to exposure that exist in tax practices through the use of electronic systems
- Explain the importance of encryption
- Implement encryption systems available for computers, smartphones, and tablets
- Explain why reuse of passwords poses an unacceptable security risk to client information
- Prepare firm procedures to improve the security of taxpayer data
- Discuss the above as well as relevant laws, regulations, and security frameworks, including the following:
  - GLBA and the FTC Safeguards Rule
  - IRS/IRC regulations/guidance relating to Cybersecurity
  - NIST Small Business Information Security—The Fundamentals

Disclaimer

This presentation along with its accompanying PowerPoint and Word documents do not constitute legal or tax advice.

AGENDA

- Introduction: Where We Are Right Now—Exposures
- Selected Cybersecurity Terms, Including Passwords and Encryption
- IRS Guidance and Regulations Relating to Cybersecurity and Protecting Taxpayer Data
- NIST's Small Business Information Security—The Fundamentals
- GLBA/FTC Rules in Detail
- A Brief Overview of Client Tax Data Confidentiality
- IRS Instructions for Reporting Website Security Incidents and Identity Theft– References/Professional Literature

In-Class Learning 1

The first step in setting up a taxpayer client data protection program should be:

a. Call the IRS service center.

b. Perform a data inventory to determine where taxpayer client data is located.

c. Contact your IT provider to identify where your users have downloaded extra copies of tax data to review outside of the workplace.

d. Consult with your local FBI office.

In-Class Learning 1: ANSWER

The first step in setting up a taxpayer client data protection program should be:

a. Call the IRS service center.

b. Perform a data inventory to determine where taxpayer client data is located.

c. Contact your IT provider to identify where your users have downloaded extra copies of tax data to review outside of the workplace.

d. Consult with your local FBI office.

Unit 1

Introduction: Where We Are Now—Exposures

KAPLAN

Introduction: Where We Are Right Now—Exposures

- Ransomware attacks involve an attacker accessing and taking control of IT systems and or files.
- The malicious attacker typically encrypts the files on the affected system, making them inaccessible to the authorized user(s).
- The attacker demands a ransom payment to restore access to the files or system.
- To date, 2021 is following in the footsteps of recent years concerning major data breaches.
- The number of impacted individuals is staggering.
- Attacks in 2021 were varied across multiple sectors.

Introduction: Where We Are Right Now—Exposures

Colonial Pipeline: Ransom Paid: $2.3 million in Bitcoin

- Colonial Pipeline, which carries 45% of the East Coast's supply of petroleum, diesel and jet fuel, was compromised by a hacking organization called DarkSide.
- The group stole nearly 100 gigabytes of data, threatening to release it to the internet unless a ransom was paid.
- As a result, U.S. gas prices rose some six cents per gallon, and many gas stations faced shortages fueled by panic buying and supply disruptions.

Introduction: Where We Are Right Now—Exposures

Reported High-Risk Security Incidents at Paid Preparers and Tax Software Providers

Number of security incidents

2017: 212

2018: 336

Number of taxpayer accounts affected

2017: 180,557

2018: 211,162

"IRS does not have a full picture of the scope of incidents because of inconsistent reporting requirements, **including no reporting requirements for paid preparers**."

Introduction: Where We Are Right Now—Exposures

Failures that lead to an unauthorized disclosure *(this includes unauthorized access through a breach*) may subject you to:

- Federal Trade Commission (FTC) sanctions
- Penalties under sections 7216 and/or 6713 of the Internal Revenue Code (I.R.C.),
- Discipline under the AICPA/state boards,
- Fines imposed by the FTC/state/non-U.S. regulators, and
- Professional liability exposure.

Introduction: Where We Are Right Now—Exposures

Gramm-Leach-Bliley Act of 1999 (GLBA), aka Financial Services Modernization Act of 1999

- IRS directs tax practitioners to the data security and data privacy requirements of the GLBA.
- Providers subject to the Gramm-Leach-Bliley Act **must** follow the FTC's Financial Privacy and Safeguards Rule.
- The Safeguards Rule requires the protection of the security, confidentiality, and integrity of customer information by implementing and maintaining a **comprehensive information security program**.
- The program **must include administrative, technical, and physical safeguards appropriate to the business's size, the nature and scope of its activities, and the sensitivity of the customer information at issue.**

The Taxpayer First Act of 2019 (TFA)

Increased penalty for improper disclosure or use of information by preparers of returns.

Impose an increased monetary penalty for the disclosure of taxpayer identity information by a return preparer in cases where such information is used in an identity theft crime, whether or not related to the filing of a tax return.

Limits tax return information redisclosures by the taxpayer's designee to only those redisclosures to which the taxpayer has expressly consented.

Requires the IRS to verify the identity of any individual opening an e-Services account before he or she is able to use such services.

Starting in 2021, all tax software providers will be required to offer multi-factor authentication options on their products that meet higher standards. Many already do so. A multi-factor or two-factor authentication offers an extra layer of protection for the username and password used by the tax professional.

Introduction: Where We Are Right Now—The Taxpayer First Act of 2019 (TFA)

Predictive policing

As the IRS increases its information-sharing activities, there may be increased application of artificial intelligence, which may allow for improved identity theft solutions and better detection of taxpayer fraud.

The IRS can be expected to use computer data analytics to more frequently identify income tax avoidance and fraud. They stated that…

"Data analytics and other technologies like 'predictive policing' help give law enforcement a clearer picture and are quickly becoming an everyday tool for CI"

With this expected increased focus from the IRS, more targeted, predictive examinations should become common practice in the near future.

Introduction: Where We Are Right Now—Exposures

Cyber liability insurance

- It is prudent to purchase standalone cyber liability insurance coverage.
- Understand coverages, requirement breach actions, notice requirements, and exclusions.
- A forensic examination of a single unauthorized release of taxpayer data could result in a several hundred thousand dollar expense.
- Many free sources of cybersecurity information and incentives are available from insurance carriers and brokers.

Introduction: Where We Are Right Now—Exposures

COVID-19

- The IRS addressed taxpayer data security concerns revolving around working from home in a series of publications titled **"Working Virtually: Protecting Tax Data at Home and** at Work."
- These publications repeat many of the concepts contained in previous publications and refer practitioners to Publications 4557 and 5293 (which we will explore in detail).
- ***Starting in 2021, all tax software providers will be required to offer multi-factor authentication options on their products that meet higher standards. In additional to tax software accounts, practitioners should use multi-factor authentication wherever it is offered.***

  For example, cloud storage providers and commercial email products offer multi-factor protections as do social media outlets. IRS e-Services is an example of an account using multi-factor authentication.

"New" FTC adopts updated Safeguards Rule

On October 27, 2021, the Federal Trade Commission (FTC) issued a final rule updating its information security rules for financial institutions' protection of consumers' financial information

The Final Rule imposes a number of new specific information security requirements on financial institutions subject to the FTC's jurisdiction.

In adopting the Safeguards Rule (2003), the FTC sought to provide financial institutions with flexibility in the implementation of their information security programs.

FTC Safeguard Rule jurisdiction

The FTC's Safeguards Rule implements this GLBA requirement, with the FTC having Safeguards Rule jurisdiction over select service providers.

This also applies to investment advisors that are not required to register with the SEC. The Final Rule slightly expands the types of financial institutions subject to the Safeguards Rule to also include "finders," which are described as companies that bring together buyers and sellers of a product or service.

- mortgage lenders
- certain non-bank lenders
- finance companies
- mortgage brokers
- account services
- check cashers
- wire transferors
- collection agencies
- credit and financial advisors
- tax preparation firms

FTC Safeguard Rule: ***New Requirements***

The Final Rule includes a limited exception for financial institutions that maintain customer information of fewer than 5,000 persons.

- Appointing a single "qualified individual" to oversee the security program
- Conducting a written risk assessment and periodically updating it.
- Implementing safeguards to control identified risks.
- Regularly testing or otherwise monitoring security controls' effectiveness.
- Implementing policies and procedures to ensure personnel are able to meet the information security program's requirements.
- Periodically assessing service providers' security risks
- Establishing a written incident response plan
- Providing annual reports

Unit 2

Selected Cybersecurity Terms

KAPLAN

Definitions of Selected Key Cybersecurity Terms

- Cybersecurity
- Privacy/Security
- Encryption
- Ransomware
- Passwords
- Reportable Breach/Security Incident
- Multi-Factor Authentication
- Personally Identifiable Information
- Taxpayer Fraud
- Social Engineering/Phishing

Data Security vs. Data Privacy

Definitions

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Data privacy is the right of a party to maintain control over and confidentiality of information about itself

Data security concerns the protection of data from accidental or intentional but unauthorized modification, destruction or disclosure through the use of physical security, administrative controls, logical controls, and other safeguards to limit accessibility.

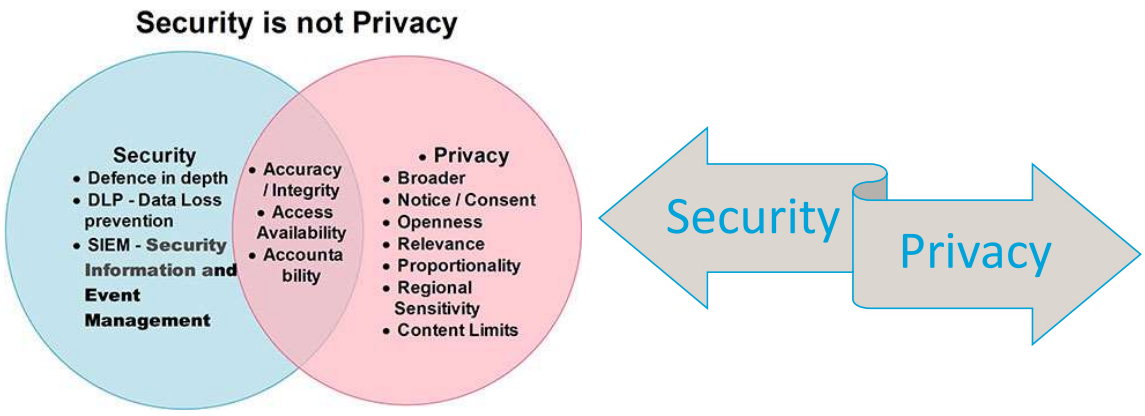
Data encryption is the converting the data into a code that cannot be easily read without a key that unlocks it.

Data masking is the masking of certain areas of data so personnel without the required authorization cannot look at it.

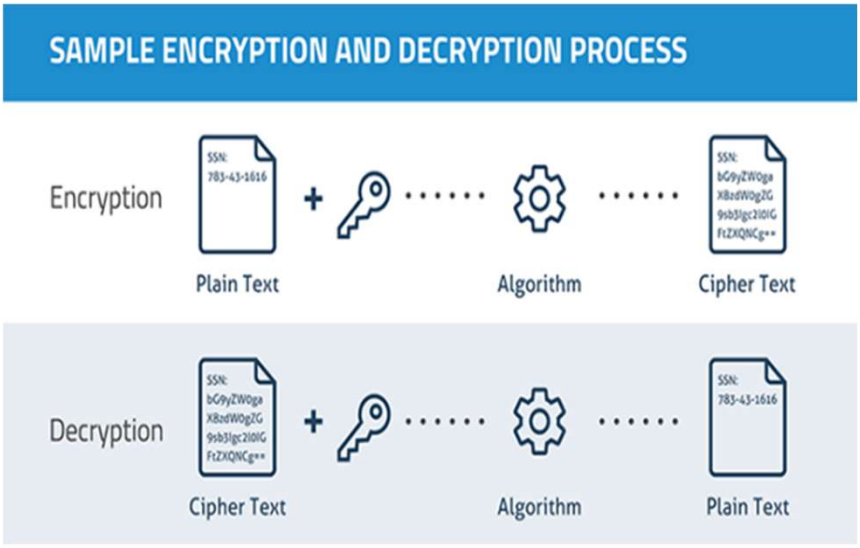
Data erasure ensures that longer used data is completely removed and cannot be recovered by unauthorized people.

Data backup involves creating copies of data so it can be recovered if the original copy is lost.

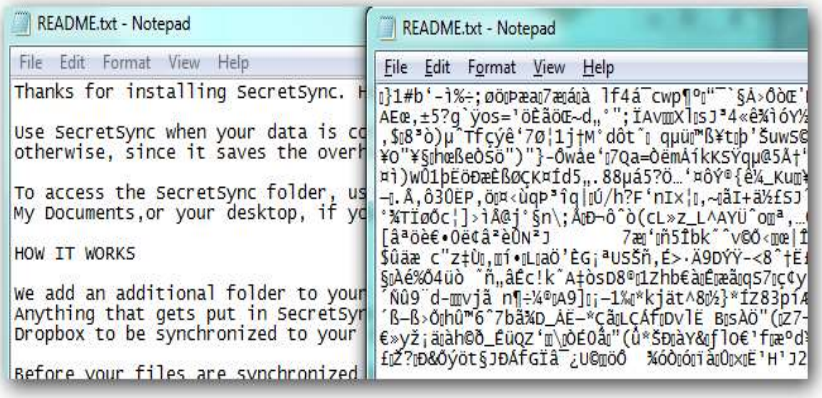
Data Security vs. Data Privacy



Encryption is the process through which legible data (plaintext) is made illegible (ciphertext) with the goal of ensuring the plaintext is only accessible by parties authorized by the owner of the data.



Encrypted Text



Encryption—When to Apply Encryption

Encryption is one piece of a broader security strategy

Encryption at rest protects your data from a system compromise or data exfiltration by encrypting data while stored.

Encryption in transit protects your data if communications are intercepted while data moves between your site and the cloud provider or between two services.

Encryption in use protects your data when it is being used by servers to run computations.

Do not forget your encryption password or key*! If you lose or forget your key, you will lose your information. Save a copy of your encryption password or key in a secure location separate from where your backups are stored.*

Encryption: Implementing Encryption Systems Available for Computers, Smartphones, and Tablets

….encrypt data or the device, or both?

Example

A well-known software encryption solution (BitLocker), when enabled, "trusted" or did nothing for encryption, under default settings, because it recognized that a hardware encryption solution had already been installed on the SSD (solid state hard drive) of a laptop computer. The laptop's hard drive encryption solution was faulty, so there was no encryption at all for data on this laptop. Unfortunately a large number of laptops were affected by this defect, but a solution was found by BitLocker's owner, Microsoft.

Walkaways….

- Always check your default settings.
- Always check for updates and bulletins published by your operating system (OS) and encryption vendors.

Encryption: Implementing Encryption Systems Available for Computers, Smartphones, and Tablets

Encryption for Mobile Devices (laptops/Tablets/Smartphones, Wearables)

- Use a Mobile Device Management (MDM) solution, which allows monitoring of all mobile devices (including the option of monitoring of BYOD). Generally, MDM can be set to monitor only work-related activity, including work-only applications, while leaving personal applications alone.
- MDM solutions allow for full-disk encryption (FDE), which encrypts the device and all of the data on it.
- Don't forget to take an inventory of all BYOD devices as well as those that are firm-issued in order to allow the MDM solution to be effective.
- When taking inventory of mobile devices, don't forget to also inventory the applications that sync to these mobile devices.
- If BYOD is limited to email only, encryption can be applied to the email and email archive, with multi-factor authentication (MFA) used as an added security tool.

Encryption: Implementing Encryption Systems Available for Computers, Smartphones, and Tablets (cont)

Encryption for Mobile Devices (laptops/Tablets/Smartphones, Wearables)

- Monitoring is critical when a mobile device has been lost or stolen—the administrator should be able to remote lock the device when the monitoring alert has been received and the employee affected reports the loss.
  - In general, the MDM solution should allow the administrator to remotely wipe the device.
  - In general, the administrator will be able to geo-locate the device.
- During normal employee use, copy/paste of firm documents and camera use can be blocked, and permissions can be applied for restricted access to selected corporate data.
- MDM can also push out OS and software/application updates to mobile devices.
- MDM solutions can be set to whitelist (accept) or blacklist (reject) applications based on a number of criteria set by the administrator.

Ransomware

Bad actors demand **Ransomware** after accessing and encrypting your data (making it inaccessible to you) while only promising to deliver the encryption key/password to you after receiving some form of payment (usually bitcoin) within a predetermined timeframe.

The attacker usually gains access through your network/webpage/app/portal, or through your vendor/subvendor's versions of these. **Sometimes the attacker will delete the victim's data or not return the encryption key even after the victim pays the ransomware funds.**

- Ensure that you regularly back up your data.
- **You may want to encrypt your backup data, but make sure you know where the encryption key or password is located.**
- Vendor oversight is extremely important in relation to ransomware situations.

Passwords: Best Practices

- IRS/NIST both require an 8-character minimum (best IT practices: 12-character minimum).
- Passphrases are better than passwords.
- Length and complexity are key concepts.
- Do not reuse the same password (using the same password for multiple purposes especially for financial logins).
- Do not reuse the same password (using the same password for multiple purposes) especially for financial logins!
- Change/refresh your passwords at a regular interval, especially for financial logins!

Passwords

Passwords

CAUTION

Worst Passwords of 2021 from NordPass (U.S.)

- Every one of the following passwords were cracked in less than a second!
- #1 was detected in 3,572081 instances!

1. 123456
2. password
3. 12345
4. 123456789
5. password1
6. abc123
7. 12345678
8. querty
9. 111111
10. 1234567

Top 200 Most Common Password List 2021 | NordPass

Password Managers

- Use a password manager to manage all of your passwords. *PC Magazine* has ranked what it considers to be the best for 2022 here: The Best Password Managers for 2022 | PCMag
- According to the tech magazine ZDNet, the advantages of using a password manager include the following:
  - ***Password generation:*** A password manager can create an immediate password that you can customize to the needs of your regulator.
  - ***Phishing protection:*** "If you visit a site that has managed to perfectly duplicate your bank's login page and even mess with the URL display to make it look legit, you might be fooled. Your password manager, on the other hand, won't enter your saved credentials, because the URL of the fake site doesn't match the legitimate domain associated with them."
  - ***Cross-platform access:*** "Password managers work across devices, including PCs, Macs, and mobile devices, with the option to sync your encrypted password database to the cloud. Access to that file and its contents can be secured with biometric authentication and 2FA."
  - ***Protection against surveillance/shoulder surfing:*** "An attacker who's able to watch you type, either live or with the help of a surveillance camera, can steal your login credentials with ease. Password managers never expose those details."

Reportable Breach/Incident

- IRS/IRC Definition:

For the purposes of this standard, an **event that can result** in an unauthorized disclosure, misuse, modification, or destruction of taxpayer information shall be considered a reportable security incident.

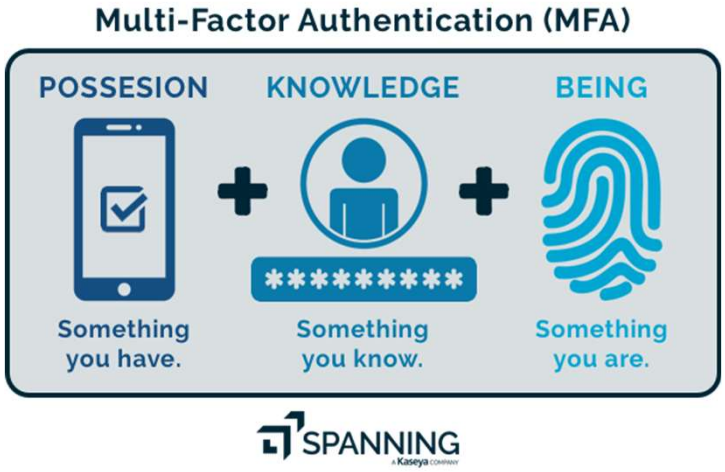
- NYDFS Definition:

Cybersecurity Event means any act or **attempt**, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

Security Event, Incident & Breach

	DEFINITION	USE CASE
Event	Single instance	• An email • A phone call • A system crash • A request for virus scans to be performed on a file or attachment
INCIDENT	Series of security events	• Violation of an explicit or implied security policy • Attempts to gain unauthorized access • Unwanted denial of resources • Unauthorized use or changes
BREACH	Intentional or unintentional release of secure or private/confidential information	• Denial of services • Viruses/Malware • Tax Fraud

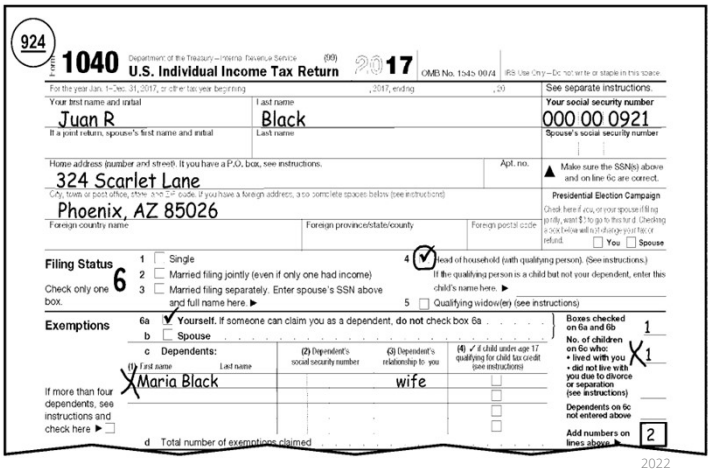
Multi-Factor Authentication (MFA)



Personally Identifiable Information (PII)

- Name
- Physical Address
- SSN
- Telephone Number
- Email Address
- IP address
- Device ID
- Browsing History

CHANGING FS 4 TO FS 6 (TY17 AND PRIOR)



Personally Identifiable Information (PII)

- **IRS/IRC Definitions**: personally identifiable information and other personal, financial, or federal tax data."
- **State definitions:** include name, email address, passport number, IP address, ID/password.
- **GLBA/FTC**: 'any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
- **NIST:** "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Personally Identifiable Information (PII)

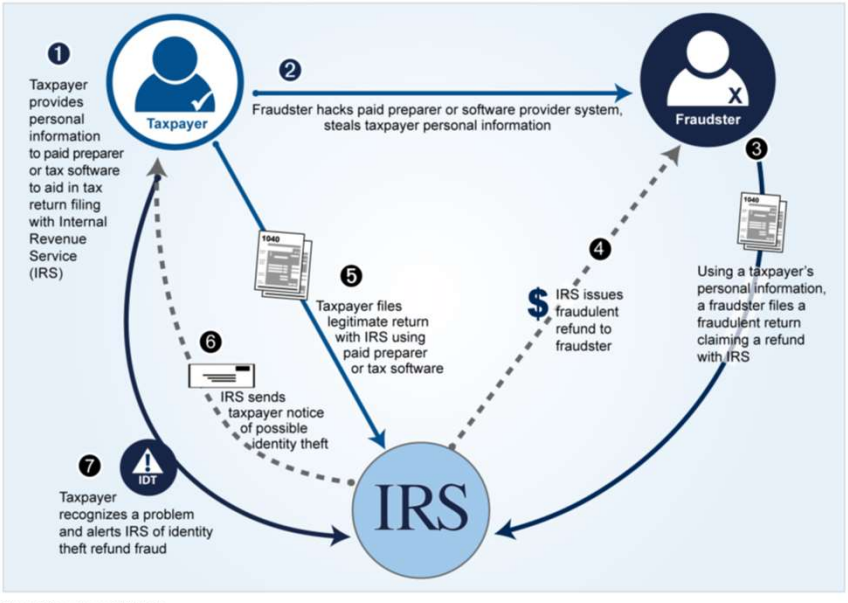
IRS Definition of tax return information

1) All the information tax return preparers obtain from taxpayers or other sources in any form or manner that is used to prepare tax returns or is obtained in connection with the preparation of returns;
2) It also includes all computations, worksheets, and printouts preparers create; correspondence from IRS during the preparation, filing, and correction of returns; statistical compilations of tax return information; and
3) Tax return preparation software registration information.

All tax return information is protected by Section 7216 and the regulations.

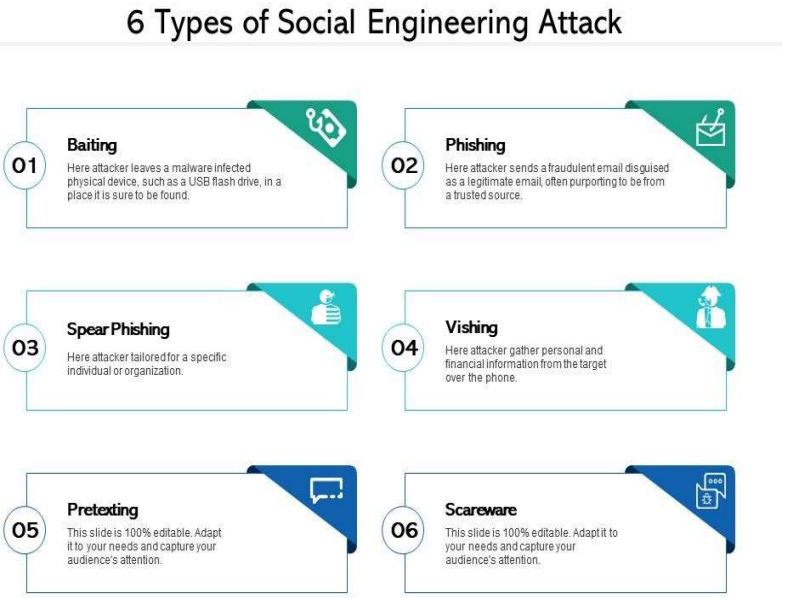
Taxpayer Fraud

Tax refund fraud consists of two crimes: (1) stealing or compromising taxpayer data and (2) using stolen (or otherwise compromised) taxpayer data to file a fraudulent tax return and collect a fraudulent refund.



Source: GAO analysis. | GAO-19-340

Social Engineering /Phishing

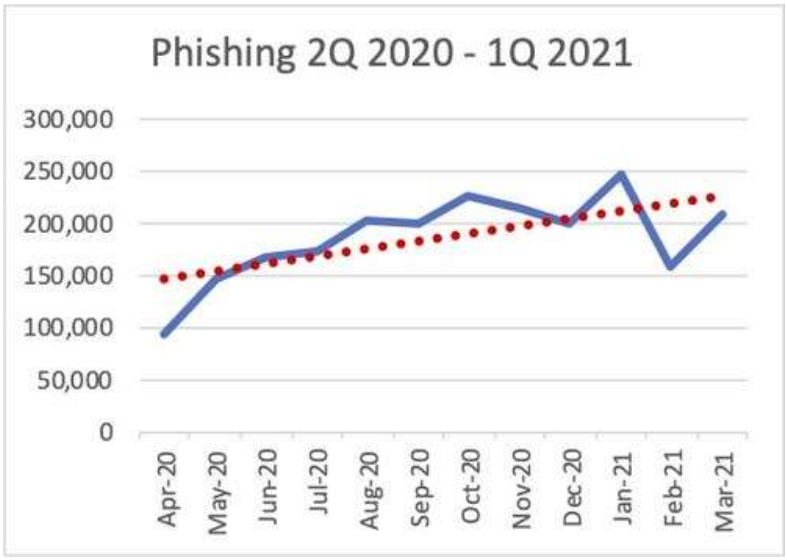


Social Engineering /Phishing

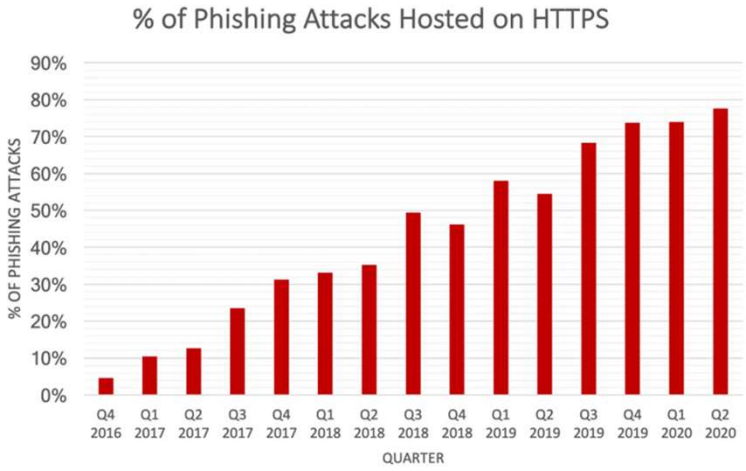
Social Engineering/Phishing

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
- Phishing is often used to gain control of an organization's networks as a part of a larger attack, such as an advanced persistent threat (APT) event.
- In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

Phishing



Phishing



Phishing

Don't click the link!

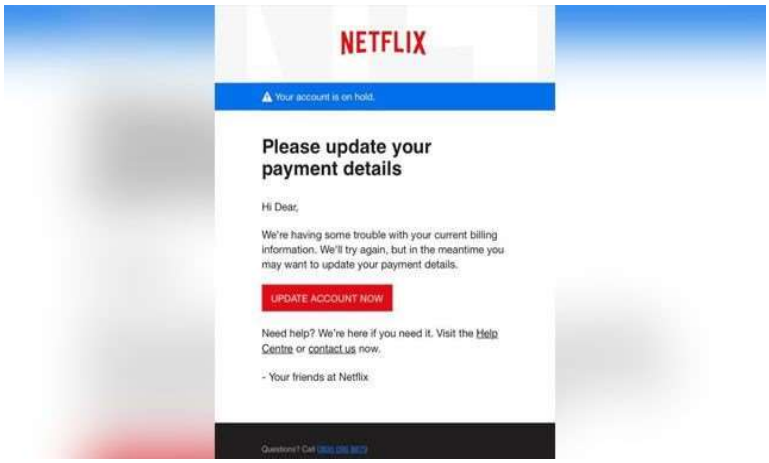
Phishing

Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam.

Attackers will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.

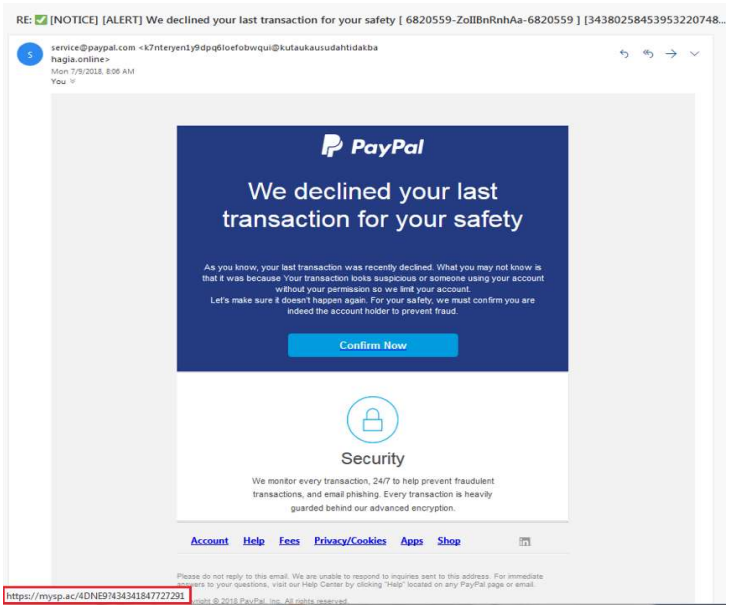
Phishing

In addition, attackers will usually try to push users into action by creating a **sense of urgency**. For example, an email could threaten account expiration and place the recipient **on a timer**. Applying **pressure** causes the user to be less diligent and more prone to error.



Phishing

Links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains.



Social Engineering

What is a vishing attack?

- Vishing is the social engineering approach that leverages voice communication.
- This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information.
- Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services.
- Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor.

Vishing

A vishing attack—*deep fake*

- Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.
- The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was **urgent**, directing the executive to pay **within an hour**. Law enforcement authorities and AI experts have predicted that criminals would use AI to automate cyberattacks.
- Whoever was behind this incident appears to have used AI-based software to successfully mimic the German executive's voice by phone. The U.K. CEO recognized his boss' slight German accent and the melody of his voice on the phone.
- It appears that attackers can use **publicly available** voice recordings to impersonate celebrities or executives.

Spear Phishing

Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

Example

1. A perpetrator researches names of employees within an organization's marketing department (LinkedIn and the external corporate website) and gains access to the latest project invoices.
2. Posing as the marketing director, the attacker emails a departmental project manager (PM) using a subject line that reads, "Updated invoice for Q3 campaigns." The text, style, and included logo all duplicate the organization's standard email template.
3. A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice.
4. The PM is requested to log in to view the document—and he does! The attacker steals his credentials, gaining full access to sensitive areas within the organization's network.

Smishing

What is a smishing attack?

Smishing is a form of social engineering that exploits SMS, or text, messages. Text messages can contain links to such things as webpages, email addresses, or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

Phishing

How to protect yourself from phishing attacks

1) Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
2) Don't send sensitive information over the internet before checking a website's security.
3) Minimize publishing sensitive firm details and information on social media (LinkedIn, Facebook, corporate website).
4) Pay attention to the Uniform Resource Locator (URL) of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

Phishing

How to protect yourself from phishing attacks

5) If you are unsure whether an email request is legitimate, try to verify it **by contacting the company directly**. Do **not** use contact information provided on a website connected to the request; instead, check previous statements for contact information.
6) Install and maintain antivirus software, firewalls, and email filters to reduce some of this traffic.
7) Take advantage of any anti-phishing features offered by your email client and web browser
8) Invest in training, which should ideally be performed for all employees, contractors, and interns upon hire and annually thereafter. At least a portion should be unannounced and should consist of distributing fake emails with links to click on. Lessons learned should be distributed to employees upon completion.

Unit 3

IRS Guidance and Regulations Relating to Cybersecurity and Protecting Taxpayer Data

KAPLAN

IRS Guidance and Regulations Relating to Cybersecurity and Protecting Taxpayer Data

- IRS Publication 4557, Safeguarding Taxpayer Data
- IRS Publication 1345 (Rev. 2-2019), Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns
- IRS Publication 5293, Data Security Resource Guide for Tax Professionals
- IR-2019-127, July 16, 2019, Tax Security 2.0—A "Taxes-Security-Together" Checklist—Steps 1–5

IRS Publication 4557, Safeguarding Taxpayer Data

IRS Publication 4557

Publication 4557 aims to assist with securing taxpayer data, including providing guidance on how to create a data security plan.

The publications review controls section requires tax practitioners to implement a baseline of IT security controls.

There are similarities with other documents we'll be reviewing, including the GLBA/FTC Safeguards Rule and NIST's Small Business Information Security publication.

IRS Publication 4557

Review internal controls

1) Install anti-malware/antivirus security software on all devices and keep software set to automatically update.
2) Use strong passwords of 8 or more characters and consider a password manager program.
3) Encrypt all sensitive files/emails and use strong password protections.
4) Back up sensitive data to a safe and secure external source not connected fulltime to a network.
5) Make a final review of return information—especially direct deposit information—prior to e-filing.
6) Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
7) Limit access to taxpayer data to individuals who need to know.
8) Check IRS e-Services account weekly for number of returns filed with EFIN.

IRS Publication 4557

Use Security Software

- **Antivirus**—prevents bad software, such as malware, from causing damage to a computer.
- **Anti-spyware**—prevents unauthorized software from stealing information that is on a computer or processed through the system.
- **Firewall**—blocks unwanted connections.
- **Drive Encryption**—protects information from being read on computers, tablets, laptops and smartphones if they are lost, stolen or improperly discarded.

Never select security software from a pop-up advertisement while surfing the web. Set security software to update automatically.

IRS Publication 4557

Create Strong Passwords

- Use a minimum of eight characters; longer is better.
- Use a combination of letters, numbers and symbols (i.e., ABC, 123, !@#).
- Change default/temporary passwords that come with accounts or devices, including printers.
- Do not reuse passwords (e.g., changing Bgood!17 to Bgood!18 is not good enough); use unique usernames and passwords for accounts and devices.
- Do not use your email address as your username if that is an option.
- Store any password list in a secure location such as a safe or locked file cabinet.
- Use a password manager program to track passwords, but protect it with a strong password.

IRS Publication 4557

Secure Wireless Networks

- Change default administrative password of your wireless router; use a strong, unique password.
- Reduce the power (wireless range) so you are not broadcasting further than you need. Log into your router to WLAN settings, advanced settings and look for Transmit (TX) power. The lower the number the lower the power.
- Change the name of your router (Service Set Identifier—SSID) to something that is not personally identifying.
- Use Wi-Fi Protected Access 2 (WPA-2) with the Advanced Encryption Standard (AES) for encryption.
- Do not use Wired-Equivalent Privacy (WEP) to connect your computers to the router; WEP is not considered secure.
- Do not use a public Wi-Fi to access business email or sensitive documents
- If firm employees must occasionally connect to unknown networks or work from home, establish an encrypted Virtual Private Networks (VPN) to allow for a more secure connection.

IRS Publication 4557

Protect Stored Client Data

- Use drive encryption to lock files and all devices.
- Backup encrypted copies of client data to external hard drives (USBs, CDs, DVDs) or use cloud storage; keep external drives in a secure location; encrypt data before uploading 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.
- Limit or disable internet access capabilities for devices that have stored taxpayer data.
- Delete all information from devices, hard drives, USBs (flash drives), printers, tablets, or phones before disposing of devices.
- Physically destroy hard drives, tapes, USBs, CDs, tablets, or phones by crushing, shredding, or burning; shred or burn all documents containing taxpayer information before throwing away.

IRS Publication 4557

Spot Data Theft

1) Client e-filed tax returns begin to reject because returns with their Social Security numbers were already filed.
2) Clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS.
3) Clients who haven't filed tax returns receive refunds.
4) Clients receive tax transcripts they did not request.
5) Clients who created an IRS online services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled; or, clients receive an IRS notice that an IRS online account was created in their names.
6) The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) exceeds number of clients.
7) Tax professionals or clients responding to emails that practitioner did not send.
8) Network computers running slower than normal.
9) Computer cursors moving or changing numbers without touching the keyboard.
10) Network computers locking out tax practitioners.

IRS Publication 4557

Monitor EFIN/PTINs

Weekly checks will help flag any abuses. Here's how:

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 PTIN.

If you have a Centralized Authorization File (CAF) number, make sure you keep your authorizations up to date. Remove authorizations for taxpayers who are no longer your clients.

IRS Publication 4557

Guard Against Phishing Emails

Educated employees are the key to avoiding phishing scams, but these simple steps also can help protect against stolen data:

- Use separate personal and business email accounts; protect email accounts with strong passwords and two-factor authentication if available.
- Install an anti-phishing tool bar to help identify known phishing sites. Anti-phishing tools may be included in security software products.
- 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; make contact first by phone, for example.
- Send only password-protected and encrypted documents if you must share files with clients via email.
- Do not respond to suspicious or unknown emails; *if IRS-related, forward to phishing@irs.gov.*

IRS Publication 4557

Be Safe on the Internet

- Keep your web browser software up to date so that it has the latest security features.
- Scan files using your security software before downloading to your computer.
- Delete web browser cache, temporary internet files, cookies and browsing history on a regular schedule.
- Look for the "S" in "HTTPS" connections for Uniform Resource Locator (URL) web addresses.
- Avoid accessing business emails or information from public Wi-Fi connections.
- Disable stored password feature offered by some operating systems.
- Enable your browser's pop-up blocker.
- Do not download files, software or applications from unknown websites.
- Note if your browser homepage changes; it could be a sign of malware or an intrusion.

IRS Publication 4557

Reporting Data Loss

1) Tax practitioners should report data losses or thefts immediately to the IRS (24 hour reporting/notification requirement)

https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts

1) Federal Bureau of Investigation, your local office (if directed by IRS).
2) Secret Service, your local office (if directed by IRS).
3) Local police—To file a police report on the data breach.
4) States in which you prepare state returns: email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
5) State Attorneys General for each state in which you prepare returns.
6) Other : Security experts, Insurance company

Respond and Recover from Data Loss

The Federal Trade Commission offers assistance to businesses who were victimized by data thefts and provides templates for letters that, for example, notify clients that a data loss has occurred. Here are some basic suggestions on how to recover from a data theft:

- Update your IRS Stakeholder Liaison with developments.
- Review FTC's Data Breach Response: A Guide for Business for helpful guidance in notifying clients and tips for responding and recovering.
- Determine how the intrusion or theft occurred and make any required fixes before resuming tax preparation activities and being issued a new Electronic Filing Identification Number (EFIN).
- Develop a continuity plan (Business Continuity Plan).
- Make full backups of all business data and files.
- Encrypt backed up files.
- Consider a monthly backup schedule, or more often during the filing season.
- Backup files after completing a routine system scan.
- Use an external hard drive or cloud storage.
- Consult with your professional insurance provider about data theft protection.

IRS Publication 1345 (Rev. 11-2020), Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns

IRS Publication 1345 Introduction

- Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*, provides rules and requirements for participation in IRS *e-file* of individual income tax returns and related forms and schedules.
- Violating a provision of this publication may subject the Authorized IRS *e-file* Provider (Provider) to sanctions.
- Providers should familiarize themselves with the Revenue Procedure 2007-40, 2007-26 I.R.B. 1488 (or the latest update) and Publication 3112, *IRS e-file Application and Participation*, to ensure compliance with requirements for participation in IRS *e-file*.
- The IRS revises Publication 1345 periodically, and the most recent version was released in October of 2021.

*Online providers must follow the **six security and privacy standards in Publication 1345**, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns.*

IRS Publication 1345

Safeguarding IRS e-file

- Safeguarding of IRS *e-file* from fraud and abuse is the shared responsibility of the IRS and Authorized IRS *e-file* Providers.
- Providers must be diligent in recognizing and preventing fraud and abuse in IRS *e-file*. Providers must report fraud and abuse to the IRS as indicated in the "Where To Get Additional Information" section.
- Providers must also cooperate with IRS investigations by making available to the IRS, upon request, information and documents related to returns with potential fraud or abuse.
- It is the legal responsibility of government, businesses, organizations, and individuals that receive, maintain, share, transmit or store taxpayers' personal information.
- Providers must appoint an individual as a Responsible Official who is responsible for ensuring the firm meets IRS e-file rules and requirements.

Taxpayer data *is defined as any information that is obtained or used in the preparation of a tax return (e.g., income statements, notes taken in a meeting, or recorded conversations). Putting safeguards in place to protect taxpayer information helps prevent fraud and identity theft and enhances customer confidence and trust.*

IRS Publication 1345

IRS e-file Security, Privacy and Business Standards

- The IRS has mandated six (6) security, privacy, and business standards to supplement the Gramm-Leach-Bliley Act to better serve taxpayers and protect their information collected, processed and stored by Online Providers of individual income tax returns.
- The security and privacy objectives of these standards are:
  - setting minimum encryption standards for transmission of taxpayer information over the internet and authentication of website owner/operator's identity beyond that offered by standard version SSL certificates;
  - periodic external vulnerability scan of the taxpayer data environment;
  - protection against bulk-filing of fraudulent income tax returns;
  - and the ability to timely isolate and investigate potentially compromised taxpayer information.

IRS Publication 1345: Security Standards

1. Extended Validation SSL Certificate*

- Online Providers of individual income tax returns shall possess a valid and current Extended Validation Secure Socket Layer (SSL) certificate using SSL 3.0/**TLS 1.0 or later** and minimum 1024-bit RSA/128-bit AES.
- *TLS 1.0 or later (most recent version is up to 1.3 as of 2022) is the preferred security standard currently in use.

IRS Publication 1345: Security Standards

2. External Vulnerability Scan

- Online Providers of individual income tax returns shall contract with an independent third-party vendor to run weekly external network vulnerability scans of all their system components in accordance with the applicable requirements of the Payment Card Industry Data Security Standards (PCIDSS).
- All scans shall be performed by a scanning vendor certified by the Payment Card Industry Security Standards Council and listed on their current list of Approved Scanning Vendors (ASV).
- The taxpayer data environment is that part of the network that possesses taxpayer data or sensitive authentication data.

IRS Publication 1345: Security Standards

3. Information Privacy and Safeguard Policies

- This standard applies to Authorized IRS *e-file* Providers participating in Online Filing of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed or stored.
- These Providers shall have a written information privacy and safeguard policy consistent with the applicable government and industry guidelines and including the following statement: "we maintain physical, electronic and procedural safeguards that comply with applicable law and federal standards." In addition, Providers' compliance with these policies shall be certified by a *privacy seal vendor acceptable to the IRS.*
- Any Privacy Seal Provider who has been identified by the Online Privacy Alliance (OPA) to meet OPA's Guidelines for Effective Enforcement of Self Regulation is acceptable to the IRS.

https://www.irs.gov/e-file-providers/privacy-seal-providers-acceptable-to-irs

IRS Publication 1345: Security Standards

4. Website Challenge-Response Test

- This standard applies to Providers participating in Online Filing of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed or stored.
- These Providers shall implement an effective challenge-response protocol (e.g., CAPTCHA) to protect their website against malicious bots.
- Taxpayer information shall not be collected, transmitted, processed or stored **unless the user successfully completes this challenge-response test.**

IRS Publication 1345: Security Standards

5. Public Domain Name Registration

- This standard applies to online providers of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed, or stored.
- These online providers shall have their website's domain name registered with a domain name registrar that is in the United States and accredited by the Internet Corporation for Assigned Names and Numbers (ICANN).
- The domain name shall be locked and not be private.

IRS Publication 1345: Security Standards

6. Reporting of Security Incidents

- Online providers of individual income tax returns shall report security incidents **to the IRS** as soon as possible **but not later than the next business day after confirmation of the incident.**
- For the purposes of this standard, **an event that can result in an unauthorized disclosure, misuse, modification, or destruction of taxpayer information shall be considered a reportable security incident.**
- In addition, if the online provider's website is the proximate cause of the incident, the online provider shall cease collecting taxpayer information via their website **immediately upon detection of the incident and until the underlying causes of the incident are successfully resolved**.

https://www.irs.gov/e-file-providers/instructions-for-reporting-web-site-security-incidents-updated-10-02-08

IRS Publication 1345

Safeguarding IRS e-file From Fraud and Abuse

- EROs must be particularly diligent while acting in their capacity as the first contact with taxpayers filing a return.
- An ERO must be diligent in recognizing fraud and abuse, reporting it to the IRS and preventing it when possible.
- Providers must cooperate with IRS investigations by making available to the IRS, upon request, information and documents related to returns with potential fraud or abuse.
- Indicators of abusive or fraudulent returns may be unsatisfactory responses to filing status questions, multiple returns with the same address, and missing or incomplete Schedules A and C income and expense documentation.

IRS Publication 1345

Verifying Taxpayer Identity and Taxpayer Identification Numbers (TINs)

- To safeguard IRS e-file from fraud and abuse, an ERO should:
  - Confirm identities and SSNs,
  - Adopted Taxpayer Identification Numbers (ATINs) and
  - Individual Taxpayer Identification Numbers (ITINs) of taxpayers, spouses and dependents listed on returns prepared by its firm.

To prevent filing returns with stolen identities, an ERO should ask taxpayers not known to them to provide two forms of identification (picture IDs are preferable) that include the taxpayer's name and current or recent address. Also, seeing Social Security cards, ITIN letters and other documents for taxpayers, spouses and dependents avoids including incorrect TINs on returns.

IRS Publication 1345

Be Aware of Non-Standard Information Documents

- The IRS has identified questionable Forms W-2 as a key indicator of potentially abusive and fraudulent returns
- EROs must always enter the non-standard form code in the electronic record of individual income tax returns for Forms W-2, W-2G, or 1099-R that are altered, handwritten or typed. An alteration includes any pen-and-ink change.
- Providers must never alter the information after the taxpayer has given the forms to them.

Refund Returns

- Providers must not direct the payment (or accept payment) of any monies issued to a taxpayer client by the government in respect of a Federal tax liability to the Provider or any firm or entity with which the Provider is associated. The IRS may sanction Providers and individuals who direct or accept such payment.

IRS Publication 1345

Direct Deposit of Refunds

- To combat fraud and identity theft, the IRS limits the number of refunds electronically deposited into a single financial account or pre-paid debit card to **three**. The fourth and subsequent refunds automatically will convert to a paper refund check and be mailed to the taxpayer.
- Providers with repeat customers or clients should check to see if taxpayers have new accounts. Some software stores prior year's information and reuses it unless it is changed. If account information is not current, taxpayers do not receive direct deposit of their refunds.
- Providers must advise taxpayers that they cannot rescind a direct deposit election and they cannot make changes to routing transit numbers of financial institutions or to their account numbers after the IRS has accepted the return. **Providers must not alter the direct deposit information in the electronic record after taxpayers have signed the tax return.**

IRS Publication 1345

Electronic Signature Guidance for Forms 8878 and 8879

Taxpayers have the option of using electronic signatures for Forms 8878 and 8879 if the software provides the electronic signature capability. If taxpayers use an electronic signature, the software and the Electronic Return Originator (ERO) must meet certain requirements for verifying the taxpayer's identity.

Electronic signatures appear in many forms and may be created by many different technologies. No specific technology is required. Examples of currently acceptable electronic signature methods include:

- A handwritten signature input onto an electronic signature pad.
- A handwritten signature, mark or command input on a display screen by means of a stylus device.
- A digitized image of a handwritten signature that is attached to an electronic record.
- A typed name (e.g., typed at the end of an electronic record or typed into a signature block on a website form by a signer).

IRS Publication 1345

Electronic Signature Guidance for Forms 8878 and 8879

- A shared secret (e.g., a secret code, password, or PIN) used by a person to sign the electronic record.
- A digital signature.
- A mark captured as a scalable graphic.

The software must record the following data:

- Digital image of the signed form.
- Date and time of the signature.
- Taxpayer's computer IP address (remote transaction only).
- Taxpayer's login identification—user name (remote transaction only).
- Identity verification: taxpayer's knowledge-based authentication passed results and for in person transactions, confirmation that government picture identification has been verified.
- Method used to sign the record, (e.g., typed name); or a system log; or other audit trail that reflects the completion of the electronic signature process by the signer.

Note: The ERO must provide this information upon request.

IRS Publication 1345

Electronic Signature Guidance for Forms 8878 and 8879

Identity Verification Requirements

- The electronic signing process must be associated with a person, and accordingly, ensuring the validity of any electronically signed record begins with identification and authentication of the taxpayer. The electronic signature process must be able to generate evidence of the person the electronic form of signature belongs to, as well as generate evidence that the identified person is actually associated with the electronic record.
- If there is more than one taxpayer for the electronic record, the electronic signature process must be designed to **separately identify and authenticate each taxpayer**.
- The identity verification requirements must be in accordance with National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guideline**, *Level 2 assurance level and knowledge-based authentication or higher assurance level*.** *(also see update at **800-63-A, on Enrollment and Identity Proofing.**

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf)

IRS Publication 1345

Electronic Signature Guidance for Forms 8878 and 8879

Identity Verification Requirements

- **Identity Assurance Levels**
  - The "strength of the assurance" with which this digital identity is mapped to and validated against a unique real-world individual is referred to in the NIST guidelines as Level of Assurance. NIST defines three levels of assurance (LOA) for the identity proofing process—1, **2** and 3—in increasing order of their strengths (IRS requires Level 2 or stronger).
- **Identity Assurance Level 2 (IAL2)**
  - For IAL2, NIST provides the following description: "*Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL2 can support IAL1 transactions if the user consents.*"
  - IAL2 allows for remote or in-person identity proofing. Example of this proofing includes services that may request an individual to prove proof of possession of an identity document, such as a Driver's License or a Passport. As part of this, collection of personally identifiable information (PII) should be kept to a minimum—only to resolve the user's identity in the context of the service that requires the identity. Also, the credential service provider may collect biometrics for the purposes of non-repudiation and re-proofing.

IRS Publication 1345

Electronic Signature Guidance for Forms 8878 and 8879

- **Identity Assurance Level 3 (IAL3)**
  - IAL3 is described in the following way: *"Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents."*
  - In essence, IAL3 is stricter than IAL2 in terms of requiring further and stronger evidence of the user's attributes so as to protect the identity and the relying party from impersonation, fraud or other such issues. Biometrics are considered mandatory as part of IAL3.

NNIST Publication 800-63-A, Identity Assurance Levels

Table 4-1 IAL Requirements Summary

Requirement	IAL1	IAL2	IAL3
Presence	No requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No requirements	The minimum attributes necessary to accomplish identity resolution. KBV may be used for added confidence.	Same as IAL2.
Evidence	No identity evidence is collected	One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence, or One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	Two pieces of SUPERIOR evidence, or One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, or Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2.
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	SP 800-53 Moderate Baseline (or equivalent federal or industry standard).	SP 800-53 High Baseline (or equivalent federal or industry standard).

IRS Publication 1345

ERO Duties After Submitting the Return to the IRS

Record Keeping and Documentation Requirements

- A copy of Form 8453, *U.S. Individual Income Tax Transmittal for an IRS e-file Return*, and supporting documents that are not included in the electronic records submitted to the IRS;
- Copies of Forms W-2, W-2G and 1099-R;
- A copy of signed IRS *e-file* consent to disclosure forms;
- A complete copy of the electronic portion of the return that can be readily and accurately converted into an electronic transmission that the IRS can process; and
- The acknowledgement file for IRS accepted returns.

Forms 8879 and 8878 must be available to the IRS *in the same manner described above for* ***three years*** *from the* ***due date of the return or the IRS received date, whichever is later. The Submission ID must be associated with Form 8879 and 8878:***

IRS Publication 1345

ERO Duties After Submitting the Return to the IRS

Disposal of Taxpayer Information

...taxpayer information and sensitive data files must be destroyed by properly shredding, burning, mulching, pulping, or pulverizing beyond recognition and reconstruction. Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller) or pulverize/ disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen.

State laws also have jurisdiction over data disposal—ensure you are familiar with these laws as well!

IRS Publication 1345

Transmission

Reporting of Potential Identity Theft Refund Fraud Activity

- **Providers who transmit more than 2,000 individual income tax returns per year are required to perform analysis to identity potential identity-theft fraud patterns and schemes, and to provide the results relative to any indicators of such fraud to the IRS on a weekly basis**, in accordance with requirements that will be distributed to providers."

IRS Publication 1345

Transmission Requirements

- Transmit all electronic portions of returns to the appropriate IRS center **within three calendar days of receipt.**
- This requirement does not apply when the IRS is not accepting specific returns, forms, or schedules until a date later than the start-up of IRS e-file due to constraints such as late legislation, programming issues and controlled validation activities, etc.
  - Controlled validation activities are when the IRS provides special instructions to transmitters relating to the submission of certain returns;
- Retrieve the acknowledgment file within two work days of transmission;
- Match the acknowledgment file to the original transmission file and send the acknowledgment file containing all conditions on accepted returns, including non-receipt of personal identification number (PIN), etc., to the electronic return originator (ERO) or intermediate service provider within two work days of retrieving the acknowledgment file;

IRS Publication 1345

Transmission Requirements

- Retain an acknowledgment file received from the IRS until the end of the calendar year in which the electronic return was filed;
- Immediately contact the IRS at its e-help number, 866-255-0654, for further instructions if an acknowledgment of acceptance for processing has not been received within two work days of transmission or if an acknowledgment for a return that was not transmitted on the designated transmission is received;
- Promptly correct any transmission error that causes an electronic transmission to be rejected;
- Contact the IRS at its e-help number, 866-255-0654, for assistance if the electronic portion of the return has been rejected after three transmission attempts;
- Ensure the security of all transmitted data;

IRS Publication 1345

Transmission Requirements

- Ensure against the unauthorized use of its Electronic Filing Identification Number (EFIN) or Electronic Transmitter Identification Number (ETIN). A transmitter must not transfer its EFIN or ETIN by sale, merger, loan, gift, or otherwise to another entity;
- Use only software that does not have an IRS assigned production password built into the software;
- Provide the Device ID from the equipment used to prepare the return

IRS Publication 1345

Disclosure of Tax Return Information

Under Treas. Reg. §301.7216-2d(1), disclosure of tax return information among Providers for the purpose of preparing a tax return ***is permissible without the taxpayer's consent****. For example, an ERO may pass on tax return information to an Intermediate Service Provider and/or a Transmitter for the purpose of having an electronic return formatted and transmitted to the IRS.*

However, if the tax return information is disclosed or used in any other way without the taxpayer's consent, an Intermediate Service Provider and/or a Transmitter may be subject to the penalties described in I.R.C. §7216 and/or the civil penalties in I.R.C. §6713 for unauthorized disclosure or use of tax return information.

In-Class Learning 2

The most common method used to successfully gain unauthorized access to a network is:

a. Tricking an employee to click on a link which will load malware that opens an executable file.

b. Brute force attacks with non-stop login attempts that use all possible combinations of keyboard characters to crack passwords.

c. Distributed Denial of Service (DDoS) attacks which use several computers to overwhelm a target website or network by overloading it with manipulated incoming data that either slows down or crashes the target over time.

d. Imposters who use fraudulent identification to enter office suites after business hours and then access desktop computers.

In-Class Learning 2: ANSWER

The most common method used to successfully gain unauthorized access to a network is:

a. **Tricking an employee to click on a link which will load malware that opens an executable file.**

b. Brute force attacks with non-stop login attempts that use all possible combinations of keyboard characters to crack passwords.

c. Distributed Denial of Service (DDoS) attacks which use several computers to overwhelm a target website or network by overloading it with manipulated incoming data that either slows down or crashes the target over time.

d. Imposters who use fraudulent identification to enter office suites after business hours and then access desktop computers.

IRS Publication 5293, Protect Your Clients; Protect Yourself Data Security Resource Guide for Tax Professionals

IRS Publication 5293

- The Financial Services Modernization Act of 1999, also known as *Gramm-Leach-Bliley Act,* requires certain entities—including tax return preparers—to create and maintain a security plan for the protection of client data.

IRS Publication 5293

Recognize phishing emails

- Create a data security plan using IRS Publication 4557.
- Use strong and unique passwords.
- Encrypt all sensitive files/emails and use strong password protections.
- Back up sensitive data to a safe and secure external source not connected fulltime to a network.
- Make a final review of return information—especially direct deposit info—prior to e-filing.
- Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
- Limit access to taxpayer data to individuals who need to know.
- Check IRS e-Services account weekly for number of returns filed with EFIN.
- Report any data thefts or losses to the appropriate IRS Stakeholder Liaison.
- Stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts, and Social Media.

IRS Publication 5293

Stay Vigilant

- Track your daily e-File acknowledgements
- Track your weekly EFIN usage.
- If you have a Centralized Authorization File (CAF) Number, make sure you keep your authorizations up to date.
- Create your IRS online accounts using the two-factor Secure Access authentication, which helps prevent account takeovers.
- Contact security expert to determine the cause and scope of the breach, to stop the breach and to prevent further breaches from occurring.
- Contact Insurance company to report the breach and to check if your insurance policy covers data breach and mitigation expenses.

IRS Publication 5293

Stay Connected

The IRS attempts to alert tax professionals as quickly as possible when it learns of a new scam, which are especially common during the filing season. Sign up so you can stay up to date with the latest alerts and tax administration issues:

- e-News for Tax Professionals—A weekly digest of important tax news geared for tax practitioners
- QuickAlerts—An urgent messaging system regarding e-File for tax professionals who have e-Services accounts.
- IRS social media—The IRS uses several social media outlets to connect with tax pros and with taxpayers.
    - Twitter.com/IRStaxpros
    - Twitter.com/IRSnews
    - Facebook.com/IRStaxpros

TAX SECURITY 2.0—
A "TAXES-SECURITY-TOGETHER"
CHECKLIST—STEPS 1-5
(IR-2019-127, JULY 16, 2019)

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 1

The initial step on the checklist involves the "Security Six" protections. These steps fall into several major security categories:

1. Antivirus software
2. Firewalls
3. Two-factor authentication
4. Backup software/services
5. Drive Encryption
6. Virtual Private Network

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 2

Create a data security plan under federal law:

- The Security Summit partners noted that many in the tax professional community do not realize they are required under federal law to have a data security plan.
- The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), gives the Federal Trade Commission authority to set information safeguard regulations for various entities, including professional tax return preparers.
- According to the FTC Safeguards Rule, tax return preparers **must create and enact security plans to protect client data**. **Failure to do so may result in an FTC investigation. The IRS also may treat a violation of the FTC Safeguards Rule as a violation of IRS Revenue Procedure 2007-40,** which sets the rules for tax professionals participating as an Authorized IRS e-file Provider.

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 2

Additional data protection provisions may apply

The IRS and certain Internal Revenue Code (IRC) sections also focus on protection of taxpayer information and requirements of tax professionals. Here are a few examples:

- **IRS Publication 3112—**IRS e-File Application and Participation
- **IRC, Section 7216—**This IRS code provision imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses information furnished to them in connection with the preparation of an income tax return.
- **IRC, Section 6713—**This code provision imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.
- **IRS Revenue Procedure 2007-40—**This legal guidance requires authorized IRS e-file providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. **It also specifies that violations of the GLB Act and the implementing rules and regulations put into effect by the FTC, as well as violations of non-disclosure rules addressed in IRC sections 6713 and 7216, are considered violations of Revenue Procedure 2007-40. These violations are subject to penalties or sanctions specified in the Revenue Procedure.**

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 3

Maintaining vigilance over the continuing threat of phishing emails

You are only as safe as your least educated employee

- More than 90% of all data thefts start with a phishing email.
- The IRS often sees tax professionals victimized after being targeted with a tactic called spear phishing.
- Common spear phishing scams seen by the IRS include thieves posing as prospective clients, sending unsolicited emails to tax professionals. After an exchange of emails, the thief sends an email with an attachment, claiming it contains the tax information needed to prepare a return. Instead, it contains spyware that allows thieves to track each keystroke.
- The IRS also sees thieves posing as tax software providers or data storage providers with emails containing links that go to web pages that mirror real sites. The thieves' goal is to trick tax professionals into entering their usernames and passwords into these fake sites, which the crooks then steal.
- Send only password-protected and encrypted documents if files must be shared with clients via email.
- Do not respond to suspicious or unknown emails; **if IRS-related, forward to phishing@irs.gov.**

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 4

Ransomware/Client data theft

- Another trick used by thieves is rather than stealing the data, they encrypt it, a practice known as ransomware. Once they encrypt the data, thieves demand a ransom in return for the code to unencrypt the data. The Federal Bureau of Investigation warns users not to pay the ransom because thieves often do not provide the code. The FBI has called ransomware attacks a growing threat to businesses and others.
- Initial signs can be as subtle as an unusually slow computer system or as obvious as multiple clients unexpectedly receiving the same IRS notice.

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 4

Recognize the signs of client data theft

The IRS and Summit partners have created a list of warning signs that a tax professional or their office may have experienced a data theft:

- Client e-filed returns begin to be rejected by the IRS or state tax agencies because returns with their Social Security numbers were already filed;
- Clients who haven't filed tax returns begin to receive taxpayer authentication letters (5071C, 4883C, 5747C) from the IRS to confirm their identity for a submitted tax return;
- Clients who haven't filed tax returns receive refunds;
- Clients receive tax transcripts that they did not request;
- Clients who created an IRS Online Services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled. Another variation: Clients unexpectedly receive an IRS notice that an IRS online account was created in their names;

https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 4

Recognize the signs of client data theft

- The number of returns filed with the tax professional's Electronic Filing Identification Number (EFIN) exceeds the number of clients;
- Tax professionals or clients responding to emails that the firm did not send;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard;
- Network computers locking out employees.

Tax Security 2.0—A "Taxes-Security-Together" Checklist—Step 5

Create a data theft recovery plan (Incident Response Plan)

Upon becoming aware of an IRS-defined security incident ("For the purposes of this standard, an **event that can result** in an unauthorized disclosure, misuse, modification, or destruction of taxpayer information shall be considered a reportable security incident"), make calling the IRS an immediate action.

Contacting the IRS and law enforcement

Contacting states in which the tax professional prepares state returns

Contacting experts (insurance carrier)

Contacting clients and other services:

- Federal Trade Commission for guidance for businesses. For more individualized guidance, contact the FTC at idt-brt@ftc.gov.
- Credit/identity theft protection agency. Certain states require offering credit monitoring and identity theft protection to victims of identity theft.
- Credit bureaus. Notifying them if there is a compromise and your clients may seek their services.
- Clients. At a minimum, send an individual letter to all victims to inform them of the breach but work with law enforcement on timing. Clients should complete IRS Form 14039, Identity Theft Affidavit, but only if their e-filed return is rejected because of a duplicate Social Security number or they are instructed to do so.

In-Class Learning 3

What term is generally defined as:

"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

a. Hacking

b. Spear Phishing

c. Cybersecurity

d. Data Privacy

In-Class Learning 3 ANSWER

What term is generally defined as:

"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

a. Hacking

b. Spear Phishing

c. Cybersecurity

d. Data Privacy

Unit 4

NIST's Small Business Information Security—
The Fundamentals

KAPLAN

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

NIST's Small Business Information Security—The Fundamentals

The National Institute of Standards and Technology (NIST) is a branch of the U.S. Commerce Department. It sets the information security framework for federal agencies. It also produced this document to provide small businesses with an overview of those steps to security data. Its focus is on five principles: ***identify, protect, detect, respond, and recover****.*

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

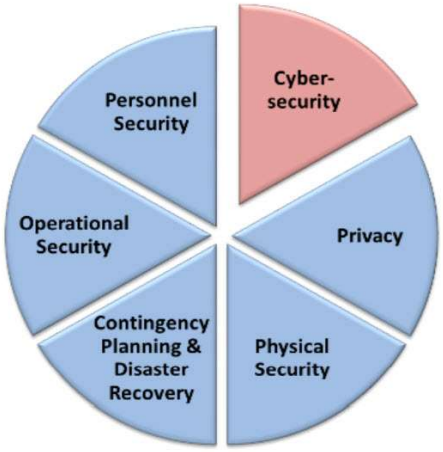
1. Background: What is Information Security and Cybersecurity?

- **Information Security** is formally defined as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" [44USC].
- **Cybersecurity** is formally defined as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation"

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

As an integral part of information security, cybersecurity works in conjunction with a variety of other security measures.

These information security components work together to provide defense against potential threats to your practice's data



NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

- **Physical Security—**the protection of property (e.g., using fences and locks);
- **Personnel Security—**(e.g., using background checks);
- **Contingency Planning and Disaster Recovery—**how to resume normal operations after an incident, also known as Business Continuity Planning;
- **Operational Security—**protecting business plans and processes; and
- **Privacy—**protecting personal information.

Lacking any one of these components diminishes the effectiveness of the others.

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

2 Understanding and Managing Your Risks

2.1 Elements of Risk

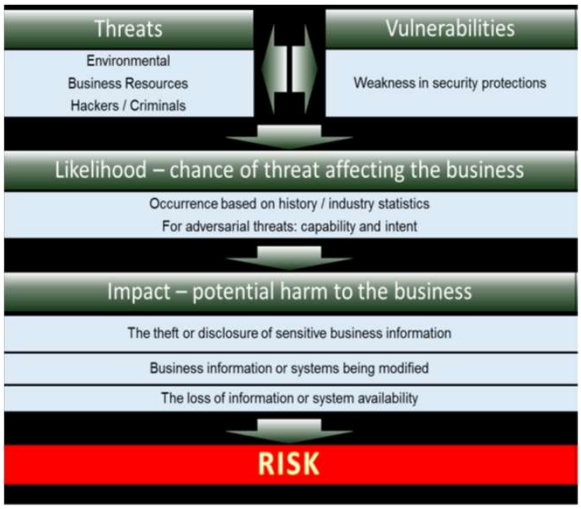
In information security, a **threat** is anything that might adversely affect the information your business needs to run. These threats might come in the form of personnel or natural events; they can be accidents, or intentional. Some of the most common information security threats include:

- **Environmental** (e.g., fire, water, tornado, earthquake);
- **Business Resources** (e.g., equipment failure, supply chain disruption, employees); and
- **Hostile Actors** (e.g., hackers, hacktivists, criminals, nation-state actors).

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

- A **vulnerability** is a weakness that could be used to harm the business. Any time or situation where information is not being adequately protected represents a vulnerability. Most information security breaches can be traced back to only a few types of common vulnerabilities.
- **Likelihood** is the chance that a threat will affect your business and helps determine what types of protections to put in place.
- The **impact** an event could have depends on the information affected, the business, and the industry.

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals
the relationship between threats, vulnerabilities, impact, and likelihood.



NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

2.2 Managing Your Risks/Performing a Risk Assessment

- The activity of identifying what information requires what level of protection, and then implementing and monitoring that protection, is called "risk management."
- You should review and update your risk management plan at least annually and whenever you may be considering any changes to the business (e.g., beginning a new project, a change in procedure, or purchasing a new IT system). Also, if you hear that something happened to one of your business partners, suppliers (including makers of any computer equipment or software you may use), customers, or employees, use this exercise to make sure you are still adequately protected.
- **Identify what information your practice stores and uses, classify it (especially sensitive/private/confidential), and know where it lives (including multiple copies/paper copies).**

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Determine the value of your information

You may not be able to assign a dollar value amount for many types of information, so instead, consider using use a scale of 0 to 3 or "none," "low," "moderate," and "high."

Using the answers to these questions, rank how critical each type of information is to the continued operations of your business.

Table 1: *Identify and Prioritize Information Types*

	Example: Customer Contact Information	Info type 1	Info type 2	Info type 3	…
Cost of revelation (Confidentiality)	*Med*				
Cost to verify information (Integrity)	*High*				
Cost of lost access (Availability)	*High.*				
Cost of lost work	*High*				
Fines, penalties, customer notification	*Med*				
Other legal costs	*Low*				
Reputation / public Relations costs	*High*				
Cost to identify and repair problem	*High*				
Overall Score:	*High*				

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Table 2: *Inventory*

	Description (e.g. nickname, make, model, serial number, service ID, other identifying information)	Location	Type of information the product comes in contact with.	Overall Potential Impact
1	*Dr. J. Smith's cell phone; Type – Sonic; Version – 9.0 ID – "Police Box"*	*Mobile T&S Network*	*Email; Calendar; Customer Contact Information; Photos; Social Media; Locations; Medical Dictionary Application*	*High*
2				
3				
4				
5				

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Table 3 provides an example of how to determine the likelihood of an incident based on the information you collected in *Tables 1 and 2*.

The left-hand column of the table lists some example threat events or scenarios—you should create a list that is specific to the threats and vulnerabilities your business faces.

Evaluate the likelihood of the threat to your business in the bottom row. Use the highest value or score given. For example, if the information type has one "high" rating, the entire information type should be rated as "high."

Table 3: *Identify Threats, Vulnerabilities, and the Likelihood of an Incident*

	Example: Customer Contact Information on Dr. J. Smith's cell phone	Info type / Technology	Info type / Technology	Info type / Technology	…
Confidentiality					
Theft by criminal	*Med (encrypted; password-protected)*				
Accidental disclosure	*Med (has previously lost phone twice)*				
Integrity					
Accidental alteration by user / employee	*Med*				
Intentional alteration by external criminal / hacker	*Low*				
Availability					
Accidental Destruction (fire, water, user error)	*Med (Regular backups)*				
Intentional Destruction	*Low*				
Overall Likelihood:	*Med*				

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

- Vulnerabilities found in software applications are the most common avenue of attack for hackers. Because of the broad range of vulnerabilities possibly found within a network or system, a vulnerability scan or analysis should be minimally conducted once a year by a professional and again whenever you make major changes to your computers or network.
- You may want to consider conducting a penetration test against your business. This test simulates an attack in order to identify weaknesses. The test should include physical, social engineering, and cyber-based attacks.
- The information gathered in *Tables 1–3* provide the information necessary to identify the areas where you need to focus your information security efforts.

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Table 4 shows an example of how the value of your information types or impact (*Tables 1 and 2*) and the potential likelihood of an attack (*Table 3*) can be combined to help you prioritize your information security efforts.

Table 4: *Prioritize Resolution Action*

Impact	High	**Priority 3** – Schedule a resolution. Focus on *Respond* and *Recover* solutions.	**Priority 1** – Implement immediate resolution. Focus on *Detect* and *Protect* solutions.
	Low	No action needed	**Priority 2** – Schedule a resolution. Focus on *Detect* and *Protect* solutions.
		Low	High
		Likelihood	

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Safeguarding Your Information

Identify

- Identify and control who has access to your business information.
- Conduct Background Checks (be aware of retaining a report or supporting documentation for this exercise—it is protected by many privacy laws).
- Require individual user accounts for each employee.
- Create policies and procedures for information security (include IRC sections as well as privacy of taxpayer data in your WISP and employee handbook).

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Safeguarding Your Information

Protect

- The Protect Function supports the ability to limit or contain the impact of a potential information or cybersecurity event.
- Limit employee access to data and information.
- Install Surge Protectors and Uninterruptible Power Supplies (UPS) (also understand the power details of your building).
- Patch your operating systems and applications.
- Install and activate software and hardware firewalls on all your business networks (Next Generation Firewalls will often include IDS/IPS).

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Safeguarding Your Information

Protect

- Secure your wireless access point and networks WPA 2.0.
- Use a VPN; Separate the Guest WiFi from the business WiFi.
- Set up web and email filters—start with enabling web filtering on your browser settings to block spam.
- Many firewalls and routers can be set up to block certain addresses (blacklist) or allow only certain addresses (whitelist). Blacklists can be downloaded online or obtained as part of a service.
- Use encryption for sensitive business information.

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Don’t forget/lose your encryption password or key!

NISTIR 7621, Revision 1
Small Business Information Security—The Fundamentals

Safeguarding Your Information

Protect

- Dispose of old computers and media safely—State laws cover data disposal, so ensure that you remove any data from your equipment before disposal.
- Train employees on the following:
  - What they are allowed to use business computers and mobile devices for, such as if they are allowed to use them to check their personal email.
  - How they are expected to treat customer or business information, for example whether or not they can take that information home with them.
  - What to do in case of an emergency or security incident (see Section 3.4).
  - How to work with, process, or handle sensitive/confidential/private taxpayer data.

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information

Detect

- Install and update antivirus, anti-spyware, and other anti-malware programs.
- Maintain and monitor logs—logs can be used to identify suspicious activity and may be valuable in case of an investigation. Logs should be backed up and saved for at least the IRS retention period of seven years.

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information

Respond

- Develop a plan for disasters and information security incidents.
- The plan should include the following:
  - **Roles and Responsibilities**. This includes who makes the decision to initiate recovery procedures and who will be the contact with appropriate law enforcement personnel.
  - **What to do with your information and information systems in case of an incident.** This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.
  - **Who to call in case of an incident**. This should include how and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers, or insurance providers. Be sure to include relevant contact information in the plan.

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information

Respond

- **Many states have notification laws, requiring you to notify customers if there is a possibility any of their information was stolen, disclosed, or otherwise lost. Make sure you know the laws for your area and include relevant information in your plans**.
- Include when to notify appropriate authorities. If there is a possibility that any personal information, intellectual property, or other sensitive information was stolen, you should contact your local police department to file a report. In addition, you may want to contact your local FBI office.

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information

Respond

- Develop a plan for disasters and information security incidents.
- The plan should include the following:
  - **Types of activities that constitute an information security incident**. This should include activities such as your business website being down for more than a certain length of time or evidence of information being stolen.
- You may want to consider developing procedures for each job role that describe exactly what the employee in that role will be expected to do if there is an incident or emergency.

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information: Recover

- The Recover Function helps an organization resume normal operations after an event.
- Make full backups of important business data/information.
- Conduct a full, encrypted backup of the data on each computer and mobile device used in your business at least once a month, shortly after a complete virus scan. Store these backups away from your office location in a protected place so that if something happens to your office (fire, flood, tornado, theft, etc.), your data is safe. Save a copy of your encryption password or key in a secure location separate from where your backups are stored.
- You can easily store backups on removable media, such as an external USB hard drive, or online using a Cloud Service Provider. If you choose to store your data online, do your due diligence when selecting a Cloud Service Provider. It is recommended that you encrypt all data prior to storing it in the Cloud.
- Test your backups immediately after generating them to ensure that the backup was successful and that you can restore the data if necessary.

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information: Recover

Make incremental backups of important business data/information.

- Conduct an automatic incremental or differential backup of each of your business computers and mobile devices at least once a week. **This type of backup only records any changes made since the last backup**. In some cases, it may be prudent to conduct backups every day or every hour depending on how much information is changed or generated in that time and the potential impact of losing that information. Many security software suites offer automated backup functions that will do this on a regular schedule for you.

These backups should be stored on:

- removable media (e.g., external hard drive);
- a separate server that is isolated from the network; or
- online storage (e.g., a cloud service provider).

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information: Recover

Make incremental backups of important business data/information.

- In general, the storage device should have enough capacity to hold data for 52 weekly backups, so its size should be about 52 times the amount of data that you have. Remember this should be done for each of your computers and mobile devices. You may choose to store your backups in multiple locations (e.g., one in the office, one in a safety deposit box across town, and one in the cloud). This provides additional security in case one of the backups becomes destroyed.
- Periodically test your backed up data to ensure that you can read it reliably. If you don't test your backups, you will have no grounds for confidence that you can use them in the event of a disaster or security incident.
- You may want to consider encrypting your backups, but don't lose the key or password!

NISTIR 7621, Revision 1 Small Business Information Security—The Fundamentals

Safeguarding Your Information: Recover

Make improvements to processes/procedures/technologies.

- Regularly assess your processes, procedures, and technology solutions according to your risks Make corrections and improvements as necessary.
- You may want to consider conducting training or table-top exercises which simulate or run-through a major event scenario in order to identify potential weaknesses in your processes, procedures, technology, or personnel readiness. Common scenarios include ransomware; key vendor collapse; successful phishing ruse.

Unit 5

GLBA/FTC Rules in Detail

KAPLAN

GLBA/FTC Rules in Detail

- The IRS directs tax practitioners to the data security and data privacy requirements of Public Law 106-102—Gramm-Leach-Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999.
- The GLBA requires "the **FTC**, along with the Federal banking agencies and other regulators, to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information. Such institutions **must develop and give notice of their privacy policies to their own customers at least annually and before disclosing any consumer's personal financial information to an unaffiliated third party, and must give notice and an opportunity for that consumer to 'opt out' from such disclosure."**
- The FTC continues to have enforcement authority. GLBA has delegated its authority to the FTC (Federal Trade Commission) in this area.

GLBA/FTC Rules in Detail

There are **four** GLBA rules covered by FTC regulations:

1) Financial Privacy
2) Safeguards
3) Red Flags (CPAs received a permanent exemption from this section in 2010)*
4) Pretexting

GLBA/FTC Rules in Detail—Privacy Rule

The Privacy Rule, which went into effect in 2000, requires a financial institution to inform customers about its information-sharing practices and allow customers to opt out of having their information shared with certain third parties.

This rule must be read within the context of IRS and AICPA regulations which cover taxpayer NPI.

What information is covered?

- The Privacy Rule protects a consumer's nonpublic personal information (NPI). NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.

GLBA/FTC Rules in Detail—Privacy Rule

NPI is:

- any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
- any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

GLBA/FTC Rules in Detail—Privacy Rule

NPI does not include information that you have a reasonable basis to believe is lawfully made publicly available. In other words, information is not NPI when you have taken steps to determine:

  - that the information is generally made lawfully available to the public; and
  - that the individual can direct that it not be made public and has not done so.
- Publicly available information includes:
  - federal, state, or local government records made available to the public, such as the fact that an individual has a mortgage with a particular financial institution; and
  - information that is in widely distributed media like telephone books, newspapers, and websites that are available to the general public on an unrestricted basis, even if the site requires a password or fee for access.

GLBA/FTC Rules in Detail—Privacy Rule

....Information in a list form may be NPI, depending on how the list is derived.

Example

A list is not NPI if it is drawn entirely from publicly available information, such as a list of a lender's mortgage customers in a jurisdiction that requires that information to be publicly recorded.

Also, it is not NPI if the list is taken from information that isn't related to your financial activities, for example, a list of individuals who respond to a newspaper ad promoting a non-financial product you sell.

GLBA/FTC Rules in Detail—Privacy Rule

A list derived even partially from NPI is still considered NPI. For example, a creditor's list of its borrowers' names and phone numbers is NPI even if the creditor has a reasonable basis to believe that those phone numbers are publicly available, because the existence of the customer relationships between the borrowers and the creditor is NPI.

Examples of Nonpublic Personal Information (in list form)

- List of a retailer's credit card customers
- List of a payday lender's customers
- List of auto loan customers merged with list of car magazine subscribers

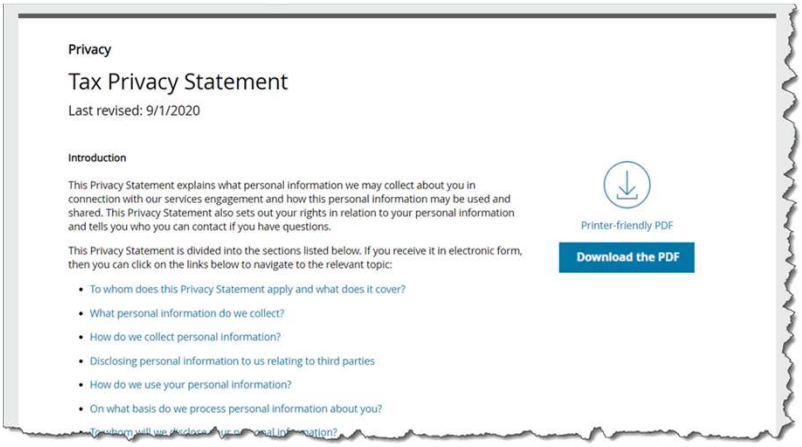
GLBA/FTC Rules in Detail—Privacy Rule

Financial institutions must give their customers—and in some cases their consumers—a "clear and conspicuous" written notice describing their privacy policies and practices. When you provide the notice and what you say depend on what you do with the information. The following are examples of web-based Privacy notices:

- Deloitte's Tax Privacy Notice for the United States: https://www2.deloitte.com/us/en/legal/tax-privacy.html
- Deloitte's Privacy Statement: https://www2.deloitte.com/us/en/legal/privacy.html
- H&R Block's Privacy Notice: https://www.hrblock.com/ffa/universal/digital-online-mobile-privacy-principles.html?otppartnerid=180
- EY Privacy Statement: https://www.ey.com/en_us/privacy-statement
- EY Cookie Policy: https://www.ey.com/en_us/cookie-policy

GLBA/FTC Rules in Detail—Privacy Rule

Deloitte's Tax Privacy Notice for the United States


Privacy

Tax Privacy Statement

Last revised: 9/1/2020

Introduction

This Privacy Statement explains what personal information we may collect about you in connection with our services engagement and how this personal information may be used and shared. This Privacy Statement also sets out your rights in relation to your personal information and tells you who you can contact if you have questions.

This Privacy Statement is divided into the sections listed below. If you receive it in electronic form, then you can click on the links below to navigate to the relevant topic:

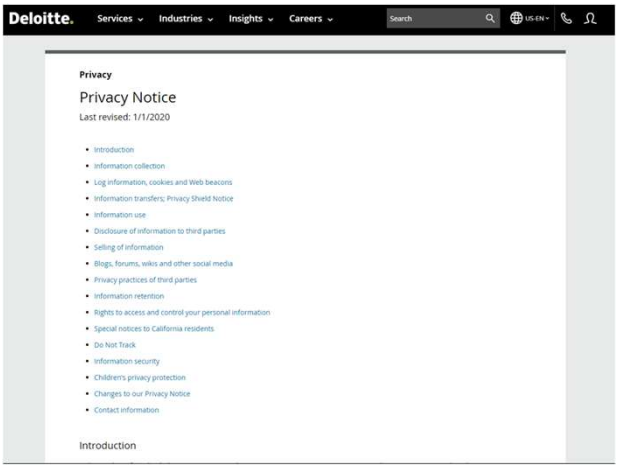
- To whom does this Privacy Statement apply and what does it cover?
- What personal information do we collect?
- How do we collect personal information?
- Disclosing personal information to us relating to third parties
- How do we use your personal information?
- On what basis do we process personal information about you?

Printer-friendly PDF

Download the PDF

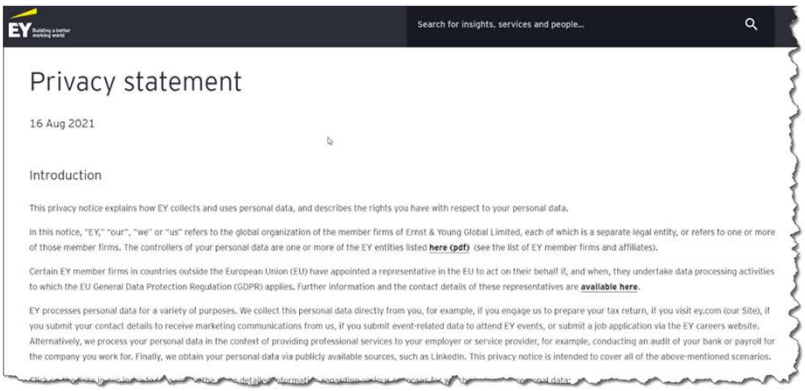
GLBA/FTC Rules in Detail—Privacy Rule

Deloitte's Privacy Statement



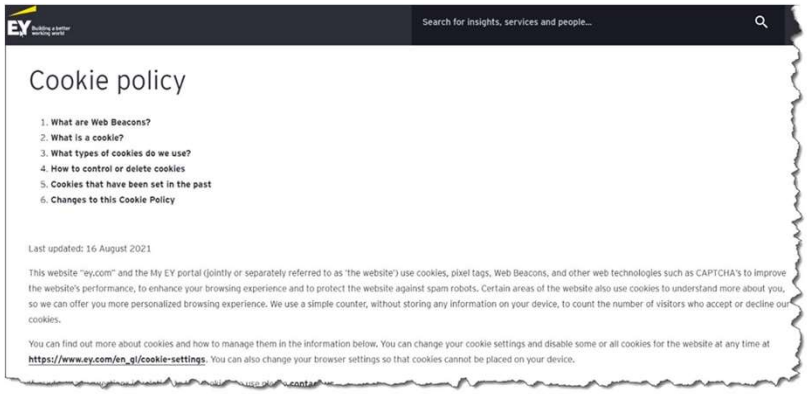
GLBA/FTC Rules in Detail—Privacy Rule

EY Privacy Statement



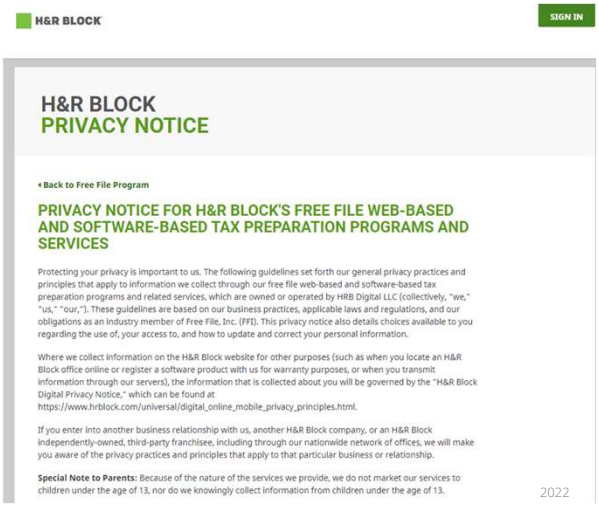
GLBA/FTC Rules in Detail—Privacy Rule

EY Cookie Policy



GLBA/FTC Rules in Detail—Privacy Rule

H&R Block's Privacy Notice



GLBA/FTC Rules in Detail—Privacy Rule

Who Gets a Privacy Notice?

- **Customers**
- Whether or not you share customer NPI, you must give all your **customers** a privacy notice.
- Under IRC Section 7216, Opt-Out Notices/Options are disallowed.
- The annual notice requirement does not apply to CPAs (Section 609 of the Financial Services Regulatory Relief Act of 2006):

  https://www.govinfo.gov/content/pkg/PLAW-109publ351/pdf/PLAW-109publ351.pdf).

The Fair Credit Reporting Act, which is included in the Privacy Rule, is not included in this course.

GLBA/FTC Rules in Detail—Privacy Rule

The Contents of the Privacy Notice

Your notice must accurately describe how you **collect, disclose, and protect NPI** about consumers and customers, including former customers. Your notice must include, where it applies to you, the following information:

- Categories of information collected. For example, nonpublic personal information obtained from an application or a third party such as a consumer reporting agency.
- Categories of information disclosed. For example, information from an application, such as name, address, and phone number; Social Security number; account information; and account balances.
- Categories of affiliates and nonaffiliated third parties to whom you disclose the information.
- Categories of information disclosed and to whom under the joint marketing/ service provider exception in section 313.13 of the Privacy Rule.

GLBA/FTC Rules in Detail—Privacy Rule

- If you are disclosing NPI to nonaffiliated third parties under the exceptions in sections 313.14 (exceptions for processing or administering a financial transaction) and 313.15 (exceptions, including fraud prevention or complying with federal or state law and others) of the Privacy Rule (see "**Exceptions**"), a statement that the disclosures are made "as permitted by law."
- Any disclosures required by the Fair Credit Reporting Act (see "Fair Credit Reporting Act"). The Fair Credit Reporting Act is not covered in this course.
- Your policies and practices with respect to protecting the confidentiality and security of NPI (see "Safeguarding NPI").

GLBA/FTC Rules in Detail—Privacy Rule

The Appearance of the Privacy Notice

1) The privacy notice must be "clear and conspicuous," whether it is on paper or on a website.
2) It must be reasonably understandable, and designed to call attention to the nature and significance of the information.
3) The notice should use plain language, be easy to read, and be distinctive in appearance.
4) A notice on a website should be placed on a page that consumers use often, or it should be hyperlinked directly from a page where transactions are conducted.

GLBA/FTC Rules in Detail—Privacy Rule

Delivering Privacy Notices

- You must deliver your privacy notices to each consumer or customer in writing, or, if the consumer or customer agrees, electronically. Your written notices may be delivered by mail or by hand. For individuals who conduct transactions with you electronically, **you may post your privacy notice on your website and require them to acknowledge receiving the notice as a necessary part of obtaining a particular product or service.**
- For annual notices, you may reasonably expect that your customers have received your notice if they use your website to access your financial products or services and agree to receive notices **at your website**, **and you post your notice continuously in a clear and conspicuous manner on your website (again, CPAs are exempted from providing annual privacy notices).**
- Notices given orally or posted in your office(s) don't comply with the rule.

GLBA/FTC Rules in Detail—Privacy Rule

Exceptions to the Notice and Opt-Out Requirements

- The section 15 exceptions apply to certain types of information-sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws. Examples of appropriate information disclosures under this exception include those made to technical service providers who maintain the security of your records; your attorneys or auditors; a purchaser of a portfolio of consumer loans you own; and a consumer reporting agency, consistent with the Fair Credit Reporting Act (see **"Exceptions"**).
- **Other than the above exceptions, IRC Section 7216 prohibits the release or sharing of taxpayer data without client consent.**

GLBA/FTC Rules in Detail—Privacy Rule

III. LIMITS ON REUSE AND REDISCLOSURE OF NPI

- **General Obligations.**
- If you receive NPI from a nonaffiliated financial institution, your ability to reuse and redisclose that information is limited. The limits depend on how the information is disclosed to you. It does not matter whether or not you're a financial institution.
- **Restrictions on Reuse and Redisclosure if NPI is Received Under the Section 14 or 15 Exceptions.**
- You may receive NPI from a nonaffiliated financial institution ("originating financial institution") under the section 14 or 15 exceptions. In these situations, you may only disclose and use the information in the ordinary course of business to carry out the purpose for which it was received. That purpose may include disclosures to other parties under the section 14 or 15 exceptions in order to carry out that activity, or as otherwise necessary, such as to respond to a subpoena (or for peer review or for a legal or regulatory requirement). You may also disclose the information to your affiliates, who are limited in their reuse and redisclosure of the information in the same way as you are, and to affiliates of the originating financial institution.

GLBA/FTC Rules in Detail—Privacy Rule

IV. DISCLOSURE OF ACCOUNT NUMBERS IS PROHIBITED

- The GLBA prohibits financial institutions from sharing account numbers or similar access numbers or codes for marketing purposes. This prohibition applies even when a consumer or customer has not opted-out of the disclosure of NPI concerning her account. The prohibition applies to disclosures of account numbers for an individual's credit card account, deposit account, or "transaction account" to any nonaffiliated third party to use in telemarketing, direct mail marketing, or other marketing through electronic mail to any consumer. A "transaction account" is any account to which a third party may initiate a charge. This provision does not prohibit the sharing of an encrypted account number, if the third party receiving the information has no way to decode it.

Additional Privacy Guidance

GAPP (Generally Accepted Privacy Principles)
(https://www.idcpa.org/writable/files/PDFs/cpa_firms_privacy_checklist.pdf

- **AICPA's Tax Identity Theft Information and Tools:** https://www.aicpa.org/interestareas/tax/resources/irsprocedureadministration/idtheftinformationandtools.html
- **Keeping clients' tax data secure, Dayna E. Roane, CPA/ABV, CGMA** October 1, 2016, https://www.journalofaccountancy.com/issues/2016/oct/how-to-secure-tax-data.html
- **Identity Theft Affidavit**: https://www.irs.gov/pub/irs-pdf/f14039.pdf

CFPB Regulation P

- In December 2015, Congress amended the GLBA as part of the Fixing America's Surface Transportation Act (FAST Act). This amendment to the GLBA provides financial institutions that meet certain conditions an exemption to the requirement under the GLBA to deliver an annual privacy notice.
- **Bureau of Consumer Financial Protection (CFPB) Updates Regulation P To Implement Legislation Amending Gramm-Leach-Bliley Act, August 10, 2018,** https://www.consumerfinance.gov/about-us/newsroom/bureau-updates-regulation-p-implement-legislation-amending-gramm-leach-bliley-act/
- As mentioned earlier, CPA firms are exempted from providing "annual privacy notices" under section 609 of the "annual notice" requirement does not apply to CPAs (Section 609 of the Financial Services Regulatory Relief Act of 2006) **but** note that other laws require covered entities to provide a Privacy Notice (usually a web-facing document with links—see Deloitte web-facing Tax Privacy Notice in the Definitions Section).

GLBA/FTC Rules in Detail—Safeguards Rule

- The Federal Trade Commission Safeguards Rule, 16 C.F.R. Part 314, requires "**financial institutions**" to ensure the **security** and **confidentiality** of consumer personal information.
- It imposes specific requirements, including the development and implementation of a written information security plan.
- **CPA firms that prepare tax returns qualify as financial institutions** under the definition contained in this rule (16 C.F.R. §313.1(b)).

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- The Safeguards Rule, which went into effect in 2003, requires financial institutions to develop, implement, and maintain a comprehensive information security program (16 CFR 314.3(a)).
- (a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
- Definition: (b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314) **Security Plan**

The Safeguards Rule requires companies to develop a **written information security plan** that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company 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 the effectiveness of the current safeguards for controlling these risks;

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314) **Securing Information**

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: employee management and training; information systems; and detecting and managing system failures. one of the early steps companies should take is to determine what information they are collecting and storing, and whether they have a business need to do so. You can reduce the risks to customer information if you know what you have and keep only what you need.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314) **Securing Information**

- Depending on the nature of their business operations, firms should consider implementing the following practices:
  - Employee Management and Training. The success of your information security plan depends largely on the employees who implement it.
- Consider:
  - Checking references or doing background checks before hiring employees who will have access to customer information.
  - Asking every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.

- Controlling access to sensitive information by requiring employees to use strong passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lowercase letters, and a combination of letters, numbers, and symbols.)

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

Using password-activated screen savers to lock employee computers after a period of inactivity.

- Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
  - Locking rooms and file cabinets where records are kept;
  - Not sharing or openly posting employee passwords in work areas;
  - Encrypting sensitive customer information when it is transmitted electronically via public networks;
  - Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
  - Reporting suspicious attempts to obtain customer information to designated personnel.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Regularly reminding all employees of your company's policy—and the legal requirement—to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
- Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
- Imposing disciplinary measures for security policy violations.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.
  Information Systems. Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:
- Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
  - Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
  - Store records in a room or cabinet that is locked when unattended.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a strong password and is kept in a physically secure area.
- Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area.
- Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Take steps to ensure the secure transmission of customer information. For example:
  - When you transmit credit card information or other sensitive financial data, **use a Secure Sockets Layer (SSL)*** or other secure connection, so that the information is protected in transit. **(TLS has superseded SSL and is highly recommended as a best practice to be used in place of SSL.)**
  - If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
  - If you must transmit sensitive data by email over the internet, be sure to **encrypt** the data.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example:
  - Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
  - Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:

- check with software vendors regularly to get and install patches that resolve software vulnerabilities;
- use antivirus and anti-spyware software that updates automatically;
- maintain up-to-date firewalls, particularly if you use a broadband internet connection or allow employees to connect to your network from home or other off-site locations;
- regularly ensure that ports not used for your business are closed; and
- promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:
  - keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
  - use an up-to-date intrusion detection system to alert you of attacks;
  - monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
  - insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
  - take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
  - preserve and review files or programs that may reveal how the breach occurred; and
  - if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.

GLBA/FTC Rules in Detail—Safeguards Rule

Safeguards (16 CFR Part 314)

- Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
  - notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
  - notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
  - notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business; and
  - check to see if breach notification is required under applicable state ***or non-U.S. law.***

** Safeguards Rule Update 2021**

- On October 27th 2021, the FTC adopted a new rules update to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses.
- In recent years, widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, and other forms of financial distress.
- The FTC's updated Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security system to keep their customers' information safe.

** Safeguards Rule Update 2021**

- The changes adopted by the Commission to the Safeguards Rule include more specific criteria for what safeguards financial institutions must implement as part of their information security program such as limiting who can access consumer data and using encryption to secure the data.
- Under the updated Safeguards Rule, institutions must also *explain their information sharing practices*, specifically the administrative, technical, and physical safeguards the financial institutions use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers' secure information.
- In addition, financial institutions will be required to *designate a single qualified individual to oversee their information security program* and report periodically to an organization's board of directors, or a senior officer in charge of information security.

** Safeguards Rule Update 2021**

- In addition to the updates, the FTC is also seeking comment on whether to make an additional change to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission.
- The FTC is issuing a supplemental notice of proposed rulemaking, which will be published in the Federal Register shortly.
- The public will have 60 days after the notice is published in the Federal Register to submit a comment.

** Safeguards Rule Update 2021**

- Lastly, the FTC also announced it adopted largely technical changes to its authority under a separate Gramm-Leach Bliley Act rule, which requires financial institutions to inform customers about their information-sharing practices and allow customers to opt out of having their information shared with certain third parties.
- These changes align the rule with changes made under the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).
- Under Dodd-Frank, Congress narrowed the FTC's jurisdiction under that rule to only apply to motor vehicle dealers.

GLBA/FTC Guidance, Start with Security, A Guide for Business, Lessons Learned from FTC Cases

Start with Security—a Guide for Business—Lessons Learned from FTC Cases, Federal Trade Commission, 2015

This document uses actual FTC cases as examples of privacy dos and don'ts.

1) *Start with Security*
2) *Control access to data sensibly*
3) *Require secure passwords and authentication*
4) *Store sensitive personal information securely and protect it during transmission*
5) *Segment your network and monitor who's trying to get in and out*
6) *Secure remote access to your network*
7) *Apply sound security practices when developing new products*
8) *Make sure your service providers implement reasonable security measures*
9) *Put procedures in place to keep your security current and address vulnerabilities that may arise*
10) *Secure paper, physical media and devices*

https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

GLBA/FTC Guidance, Start with Security, A Guide for Business, Lessons Learned from FTC Cases

1. Start with Security

- Factor it into the decision making in every department of your business—HR, sales, accounting, information technology, operations, legal.
- Data collection, retention, and use policies (have a rationale/legitimate business need—statutory requirement/best practices, etc.).
- Don't collect personal information you don't need.
- Retain indefinitely? NO

GLBA/FTC Guidance, Start with Security, A Guide for Business, Lessons Learned from FTC Cases

2. Control access to data sensibly

- Put controls in place to make sure employees have access only on a "need to know" basis
- For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases
- For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet
- **Restrict access to sensitive data**.
- **Limit administrative access**
- Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

3. Require secure passwords and Authentication

- Insist on complex and unique passwords
- Store passwords securely
- Guard against brute force attacks—lock out user access after unsuccessful attempts
- Protect against authentication bypass—test for common vulnerabilities

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

4. Store sensitive personal information securely and protect it during transmission

- Keep sensitive information secure throughout its lifecycle—encrypt data
- Use industry-tested and accepted methods—ValueClick
- Ensure proper configuration—SSL used (TLS version 1.0 or higher is preferred)

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

5. Segment your network and monitor who's trying to get in and out

- Segment your network
- Monitor activity on your network

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

6. Secure remote access to your network

- Ensure endpoint security
- Put sensible access limits in place

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

7. Apply sound security practices when developing new products

- Train your engineers in secure coding
- Follow platform guidelines for security—don't turn off recommended security settings
- Verify that privacy and security features work
- Test for common vulnerabilities—look out for known vulnerabilities (OWASP)
  - The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
  - https://owasp.org/www-project-top-ten/

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

8. Make sure your service providers implement reasonable security measures

- Put it in writing
- Verify compliance

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

9. Put procedures in place to keep your security current and address vulnerabilities that may arise

- Update and patch third-party software
- Heed credible security warnings and move quickly to fix them

GLBA/FTC Guidance: Start with Security: A Guide for Business—Lessons Learned from FTC Cases

10. Secure paper, physical media, and devices

- Securely store sensitive files
- Protect devices that process personal information
- Keep safety standards in place when data is en route
- Dispose of sensitive data securely

In-Class Learning 4

Which of the steps below are elements of the IRS "Security Six" protections mentioned in the Tax Security 2.0 "Taxes-Security-Together" Checklist?

a. Antivirus
b. Firewalls
c. Two-Factor Authentication
d. Backup software/services
e. All of the above

In-Class Learning 4 ANSWER

Which of the steps below are elements of the IRS "Security Six" protections mentioned in the Tax Security 2.0 "Taxes-Security-Together" Checklist?

a. Antivirus

b. Firewalls

c. Two-Factor Authentication

d. Backup software/services

e. All of the above

Unit 6

Confidentiality of Client Tax Data,
Selected Guidance, Rulings, and Laws

KAPLAN

Confidentiality of Client Tax Data

Confidentiality Restrictions

Generally, a practitioner is prohibited from disclosing client taxpayer data without client consent. Applicable resources include….

- IRC sections include Section 7216, 7602, 7525, and 6713;
- relevant case law;
- Circular 230 Section 10.29;
- and, for CPA practitioners, also see AICPA Code of Professional Conduct, Section 1.700.001(.005 through.100).

Confidentiality of Client Tax Data

Third-party disclosure

Disclosure pursuant to a court order is excluded, but a mere discovery request or subpoena duces tecum issued by an attorney does not qualify. The wording of the client's consent form is important, because the statute specifies that each separate use or disclosure must have an individual consent.

A CPA whose client will not consent in writing to the disclosure may be wise to tell the requesting party to obtain a court order.

https://www.cpajournal.com/2017/03/20/applying-aicpas-professional-standards-tax-practice/

Confidentiality of Client Tax Data

Third-party disclosure

*In **Robert v. Chaple** [369 S.E. 2d 482 (Ga. App. 1988)], the court held that a CPA's disclosure to the IRS under an informal request violated IRC section 7216. The prudent position would seem to be to wait for the IRS certificate, unless the client consents in writing.*

When multiple parties are preparing an electronic return, a provider, including an electronic review organization (ERO), may disclose tax return information to other providers relating to an e-filing a tax return under Treas. Regulation Section 301.7216-2(d)(1) without obtaining the taxpayer's consent.

Example

*An ERO may pass on return information to an intermediate service provider or a transmitter for the purpose of having an electronic return formatted or transmitted to the IRS. **AICPA guidance states that consent forms should be used in this situation.***

Confidentiality of Client Tax Data

Tax advice privilege

- The 1998 IRS Restructuring and Reform Act created a tax advice attorney-client privilege under IRC section 7525, applicable to "federally authorized tax practitioners."
- The privilege is limited, however, to non-criminal, nontax shelter related tax proceedings.
- Tax preparation information in a criminal tax case is also excluded from the privilege, even if accompanied by tax advice.
- Dual-purpose documents are not privileged, so separate files are a necessity [see *U.S. v. Fredrick*, 182 F 3d 496 (7th Cir. 1999)]. This privilege does not apply to civil litigation or any non-IRS proceeding.

Confidentiality of Client Tax Data

Tax advice privilege

- The IRS allows a limited tax advice attorney-client privilege available to certain tax practitioners.
- The 1998 IRS Restructuring and Reform Act created a tax advice attorney-client privilege under IRC section 7525, applicable to "federally authorized tax practitioners."
- The privilege is limited, however, to non-criminal, nontax shelter related tax proceedings. Tax preparation information in a criminal tax case is also excluded from the privilege, even if accompanied by tax advice.
- Dual-purpose documents are not privileged, so separate files are a necessity [see U.S. v. Fredrick, 182 F 3d 496 (7th Cir. 1999)]. This privilege does not apply to civil litigation or any non-IRS proceeding
- Clients must have an expectation that a tax communication was to be kept confidential. Any inadvertent disclosure to the IRS may waive the privilege, however [see *IBM v. IRS,* 37 Fed. Cl. 599 (1997)]. This privilege does not apply to civil litigation or any non-IRS governmental proceedings.

Confidentiality of Client Tax Data

IRC Section 7216

Section 7216 applies to tax return information, which is any information that is furnished for, or in connection with, the preparation of a return (or amended return) of income tax imposed under chapter 1 of the Internal Revenue Code. Tax return information may be publicly available, but it would still be protected as tax return information by virtue of its being supplied as part of a tax return engagement.

Practitioners should be aware that Section 7216 *supersedes* the information sharing sections of the FTC/GLBA Privacy Rule

Internal Revenue Code Sec. 7216 is a criminal provision enacted by the U.S. Congress in 1971 that prohibits preparers of tax returns from knowingly or recklessly disclosing or using tax return information. A convicted preparer may be fined not more than $1,000 ($100,000 in the case of a disclosure or use to which section 6713(b) applies), or imprisoned not more than one year or both, for each violation.

IRC Section 7216/AICPA

Consent Forms

Consent forms should be used when tax return information is shared with outside parties including entities related to a tax practitioner's firm, such as:

- *an affiliated investment advisory or wealth management firm*
- *or with another tax practitioner who is assisting with the preparation of the return if that practitioner is not part of or employed by the firm that is preparing the return.*

The appropriate consent forms for one accounting firm may not be suitable for another firm.

Each tax preparer should read…

- *Regs. Sec. 301.7216,*
- *Rev. Proc. 2013-14 and*
- *Rev. Proc. 2013-19*

…very closely when drafting the appropriate consent forms necessary to meet the unique facts and circumstances of his or her firm's needs.

AICPA Ethics

Confidential Client Information Rule under Section 1.700.001

391/Interpretation 391-2, "Disclosure of Client Information to Third Parties"

Regs. Secs. 301.7216-1 through 301.7216-3

1.700.005, "Application of the Conceptual Framework for Members in Public Practice and Ethical Conflicts";

1.700.010, "Client Competitors";

1.700.020, "Disclosing Information From Previous Engagements";

1.700.030, "Disclosing Information to Persons or Entities Associated With Clients";

1.700.040, "Disclosing Information to a Third-Party Service Provider";

AICPA Code of Professional Conduct, Section 1.700.001

Confidential Client Information Rule under Section 1.700.001

- 1.700.050, "Disclosing Client Information in Connection With a Review of the Member's Practice";
- 1.700.060, "Disclosure of Client Information to Third Parties";
- 1.700.070, "Disclosing Client Information During Litigation";
- 1.700.080, "Disclosing Client Information in Director Positions";
- 1.700.090, "Disclosing Client Names"; and
- 1.700.100, "Disclosing Confidential Client Information as a Result of a Subpoena or Summons."

Unit 7

IRS Instructions for Reporting Website Security Incidents and Identity Theft

KAPLAN

IRS Instructions for Reporting Website Security Incidents

- Keep in mind that you will probably be required to report security incidents or breaches **to additional state and regulatory bodies in addition to the IRS**! Confirm your reporting requirements with your attorney on a periodic basis as state laws in this area are constantly evolving.
- **For example**, a security incident (let's say an unsuccessful attempt at access to your client data that was discovered by your cloud vendor) in New York State may require you to report the incident to:
  - Within 24 hours, (IRS notification timeline) to the IRS;
  - Within 72 hours, to the New York Department of Financial Services;
  - Within 24 hours (IRS Deadline) to the New York State Tax authorities; and
  - Within 10 days to the New York State Attorney General, the State Police, and the Department of State (State Secretary of State).

IRS Instructions for Reporting Website Security Incidents

www.irs.gov/e-file-providers/instructions-for-reporting-web-site-security-incidents-updated-10-02-08

Updated 10/8/2021

Submit a Microsoft Excel spreadsheet, or a Microsoft Word document, that has been encrypted using WINZIP 9 with password protection. The submission must include the following information:

1. Date and time of the incident.
2. Source of the incident.
3. Method of detection.
4. Detail description of the incident.
5. Why should the incident be of concern.
6. Corrective actions planned or taken.
7. Whether taxpayer information was disclosed (Y/N only, do not include taxpayer information).
8. Number of taxpayers impacted.
9. Regular business hours contact name, phone number, and e-mail address.
10. After-hours contact name, phone number, and e-mail address.
11. Provider's EFIN.

    and

12. The name of a Principal or Responsible Official as shown on the e-file application.

Note: This information must be enumerated exactly as above.

Submit the ZIP file and the password to new.efile.requirements@irs.gov via two separate email messages.

The Subject line of both email messages must show **SECURITY INCIDENT**.

Reporting Identity Theft

Identity Theft Affidavit

- https://www.consumer.ftc.gov/blog/2018/04/new-way-report-tax-identity-theft
- https://www.irs.gov/newsroom/when-to-file-a-form-14039-identity-theft-affidavit
- https://www.irs.gov/pub/irs-pdf/f14039.pdf

Professional Literature

- https://www.irs.gov/pub/irs-pdf/p4557.pdf, *Safeguarding Taxpayer Data: A Guide For Your Business*
- https://www.irs.gov/pub/irs-pdf/p1345.pdf, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*
- https://www.irs.gov/pub/irs-pdf/p5293.pdf, *Protect Your Clients; Protect Yourself ,Data Security Resource Guide for Tax Professionals, Catalog Number 71256E*
- https://www.irs.gov/individuals/data-theft-information-for-tax-professionals, *Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 2-2019)*
- *https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1*

Professional Literature

- https://www.irs.gov/e-file-providers/instructions-for-reporting-web-site-security-incidents-updated-10-02-08
- https://www.gao.gov/assets/700/699000.pdf. United States Government Accountability Office (GAO), TAXPAYER INFORMATION, IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices, GAO-19-340, May 2019
- Gramm-Leach-Bliley Act, Pub. L. No. 106-102, title V, 113 Stat. 1338, 1436-50 (Nov. 12, 1999), *codified at* 15 U.S.C. §§ 6801–6827;
- Federal Trade Commission Safeguards Rule, 16 C.F.R. pt. 314; Department of the Treasury, https://www.ecfr.gov/current/title-16/part-314
- https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Professional Literature

- https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm
- https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act
- Internal Revenue Service Pub. 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* (Rev. 2-2019);
- Department of the Treasury, Internal Revenue Service Pub. 3112, *IRS* e-file *Application and Participation,* (Rev. 7-2018)
- https://www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals
- https://www.irs.gov/newsroom/tax-scams-consumer-alerts
- https://www.journalofaccountancy.com/news/2019/oct/tigta-irs-challenges-2020-201922284.html
- Revenue Procedure 2007-40

Professional Literature

- https://www.treasury.gov/tigta/management/management_fy2020.pdf
- https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf
- https://www.us-cert.gov/ncas/tips/ST04-014 (Avoiding Phishing Attacks)
- https://www.tripwire.com/state-of-security/security-data-protection/phishing-campaign-used-subpoena-themed-email-to-deliver-infostealer/ (Phishing campaign which uses a realistic subpoena theme through a link to Microsoft and Google services/documents
- https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html
- **The Gramm-Leach-Bliley Act still applies to CPAs,** posted by AICPA Communications on Nov 21, 2017, https://blog.aicpa.org/2017/11/the-gramm-leach-bliley-act-still-applies-to-cpas.html#sthash.f9vP7qwS.dpbs
- **Forgot password? Five reasons why you need a password manager, Ed Bott for the Ed Bott Report, February 7, 2019,** https://www.zdnet.com/article/ forgot-password-five-reasons-why-you-need-a-password-manager

Reminders

❑**Post event evaluation:** Please complete the course evaluation that will be pushed out to you as a pop up link on your screen. We welcome your feedback!


KAPLAN