



ACCOUNTING

CONTINUING EDUCATION

Protecting Tax Information— Cyber-Security for the Tax Professional (PTIC4)

Protecting Tax Information— Cyber-Security for the Tax Professional

(PTIC4)

Tom Gancarski, CPA



PROTECTING TAX INFORMATION—CYBER-SECURITY FOR THE TAX
PROFESSIONAL (PTIC4)

©2022 Kaplan, Inc.

Published in 2022 by Kaplan Financial Education.

Printed in the United States of America.

All rights reserved. The text of this publication, or any part thereof, may not be translated, reprinted or reproduced in any manner whatsoever, including photocopying and recording, or in any information storage and retrieval system without written permission from the publisher.

ISBN: 978-1-0788-1421-8

TABLE OF CONTENTS

UNIT 1

Introduction: Where We Are Right Now—Cybersecurity Exposures for Tax Practitioners	1
Learning Objectives	1
Knowledge Level.....	1
Where We Are Right Now: Exposures	2
The Taxpayer First Act of 2019 (TFA)	4
“New” FTC Adopts Updated Safeguards Rule.....	6

UNIT 2

Selected Cybersecurity Terms	15
Learning Objective	15
Cybersecurity Terms.....	15
Cybersecurity	15
Privacy & Confidentiality	16
Encryption	16
Encryption: Implementing Encryption Systems Available for Computers, Smartphones & Tablets.....	19
Ransomware.....	21
Passwords	21
Reportable Breach/Security Incident	22
Multi-Factor Authentication	22
Personally Identifiable Data/Taxpayer Data.....	22
Antivirus	23
Taxpayer Fraud.....	25
Social Engineering	26

UNIT 3

IRS Guidance & Regulations Relating to Cybersecurity & Protecting Taxpayer Data.....	37
Learning Objectives	37
IRS Publications.....	37
IRS Publication 1345 (Rev. 10-2021), Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns	48
IRS Publication 5293, Protect Your Clients; Protect Yourself; Data Security Resource Guide for Tax Professionals	61
Tax Security 2.0—A “Taxes-Security-Together” Checklist—Steps 1-5 (IR-2019-127, July 16, 2019)	66

UNIT 4

NIST’s Small Business Information Security—The Fundamentals.....	77
Learning Objectives	77
NIST’s Small Business Information Security—The Fundamentals	77
Understanding & Managing Your Risks	79

UNIT 5

GLBA/FTC Rules in Detail	91
Learning Objectives	91
The Privacy Rule.....	92
Obligations Under the Privacy Rule	93
Limits on Reuse & Redisclosure of NPI	100
Disclosure of Account Numbers Is Prohibited.....	100
Safeguards Rule	101
Security Plan.....	102
Securing Information	103
Start with Security: A Guide for Business—Lessons Learned from FTC Cases.....	108

UNIT 6

Confidentiality of Client Tax Data	111
Learning Objective	111
Confidentiality Restrictions.....	111

UNIT 7

IRS Instructions for Reporting Website Security Incidents & Identity Theft	115
Learning Objective	115
Professional Literature	121

Unit 1

Introduction: Where We Are Right Now—Cybersecurity Exposures for Tax Practitioners

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Discuss** the current cybersecurity situation relating to tax practitioners and similarly situated businesses as cyberattacks are becoming a common occurrence and have been increasing in numbers.
- ☐ **Review** the basic/minimum requirements that the IRS and the FTC place on tax practitioners as well as the penalties and fines levied for non-compliance (details follow in later units).
- ☐ **Explain** why purchasing cyber liability insurance coverage may be a good idea.

Today, we are engaged in an escalating war against thieves, rogues, and generally bad people who want to steal our data. Every few months, we learn that a new record amount of personal information has been stolen in a hacking incident that the victim firm “just became aware of.” As a tax practitioner, you certainly don’t want to be in the news for a breach. The Internal Revenue Service (IRS) and the Federal Trade Commission (FTC), along with state and industry-specific regulators, require tax practitioners to put minimum security and privacy controls in place to protect taxpayer personal data. We will discuss these requirements throughout this course, and you will see some overlap among the guidance documents, laws, and best practices. First, we’ll start with a high-level overview of where we are right now in this cybersecurity war.

KNOWLEDGE LEVEL

This course requires a basic knowledge of cybersecurity and information technology as well as a thorough understanding of both what comprises taxpayer data and the compliance requirements for taxpayer confidentiality.

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.¹

To date, 2021² is following in the footsteps of recent years concerning major data breaches. The number of affected individuals is staggering. Attacks in 2021 were varied across multiple sectors. In particular, the Colonial Pipeline breach is especially unnerving because this was a direct attack on our supply chain, resulting in a threat to national security.

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 6 cents per gallon, and many gas stations faced shortages fueled by panic buying and supply disruptions.

Facebook, Instagram and LinkedIn via Socialarks: Records Breached: 214 million

Tens of millions of Facebook, Instagram, and LinkedIn profiles have been exposed by a company you've probably never heard of: Socialarks. Due to an unsecured database, the quickly growing Chinese social media management company leaked personally identifiable information (PII) of some 214 million social media users, some of whom were major influencers and celebrities.

Bonobos: Records Breached: 7 million

In January 2021, notorious hacker ShinyHunters struck again, this time at men's clothing retailer Bonobos. The cybercriminal made away with the PII of more than 7 million shoppers, which included their addresses, phone numbers, and account information, plus 3.5 million partial credit card numbers. The stolen data were discovered in a forum for hackers, given away for free.

Kroger via Accellion: Records Breached: 1,474,284

It's not often we think of grocery stores as targets for a healthcare hack, but that's exactly what happened to supermarket mogul Kroger. In February 2021, a breach at third-party cloud provider Accellion opened the door for hackers, giving them unfettered access to Kroger's Human Resources data and pharmacy records. Although the company claims that only 1% of its customers were affected, the breached records included sensitive information, such as names, phone numbers, home addresses, dates of birth, Social Security numbers, prescriptions, and health insurance information.

¹ Cybersecurity and Infrastructure Security Agency (CISA), <https://www.us-cert.gov/Ransomware>

² <https://www.bluefin.com/bluefin-news/2021-biggest-data-breaches-so-far/>

Volkswagen & Audi: Records Breached: 3.3 million

An unnamed marketing services company is responsible for the breach of 3.3 million Volkswagen and Audi customers and prospects in Canada and the U.S., thanks to data left unsecured. The vulnerable data, collected between the years of 2014 and 2019, were accessed by an unauthorized party in March. The sensitivity of the information varied from makes and models of vehicles that had been purchased or inquired about to a smaller number of breached Social Security numbers, tax IDs, loan numbers, and driver's license numbers.

Reported High-Risk Security Incidents at Paid Preparers & Tax Software Providers, 2017 & 2018:

Number of security incidents:

■ 2017: 212

■ 2018: 336

Number of taxpayer accounts affected:

■ 2017: 180,557

■ 2018: 211,162³

"{The} IRS does not have a full picture of the scope of incidents because of inconsistent reporting requirements, including no reporting requirements for paid preparers."⁴

As noted, safeguarding taxpayer data is a top priority for the IRS. It is the legal responsibility of government, businesses, organizations, and individuals that receive, maintain, share, transmit, or store taxpayers' personal information. **Taxpayer data** is defined as any information that is obtained or used in the preparation of a tax return or tax-related services. Failing to take necessary steps to implement or correct your security program may result in FTC sanctions (we'll cover the FTC security program requirements in a separate chapter). In addition, fines and regulatory action may also be levied by additional federal and state entities, including the IRS.⁵

Practitioners who knowingly or recklessly disclose or use tax return data may be subject to penalties under sections 7216 and/or 6713 of the Internal Revenue Code (IRC); discipline under the AICPA state boards; fines imposed by the FTC, state, or non-U.S. privacy regulators; and may be subject to professional liability exposure. For example, the New York State Department of Financial Services' (NYDFS) cybersecurity statute defines *attempted access* as a reportable incident (which may result in an adverse action from NYDFS).

³ GAO-19-340 Taxpayer Information.

⁴ GAO-19-340 Taxpayer Information.

⁵ <https://www.irs.gov/tax-professionals/summary-of-preparer-penalties-under-title-26>, ethical violations; <https://www.cnbc.com/2016/11/25/what-to-do-when-your-tax-preparer-screws-up.html>, and state data privacy, security, breach law.

According to the IRS, safeguarding of IRS e-file data from fraud and abuse is the shared responsibility of the IRS and authorized IRS e-file providers (the term *practitioners* will also encompass *providers*, but occasionally the term *providers* will be used for specific e-filer responsibilities). Providers must be diligent in recognizing and preventing fraud and abuse in IRS e-file. Also, providers must report fraud and abuse to the IRS as indicated in the "Where to Get Additional Information" section (also see the final section of this course for fraud reporting details). 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.⁶

The IRS directs tax practitioners to the data security and data privacy requirements of Public Law 106-102 of the Gramm-Leach-Bliley Act—of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999.

Practitioners subject to the GLBA must follow the FTC's Financial Privacy and Safeguard (Security) Rules. The Safeguard Rules require 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 (details appear in a later section).⁷

THE TAXPAYER FIRST ACT OF 2019 (TFA)

The TFA was signed into law by President Trump on July 1, 2019 with these cybersecurity and confidentiality requirements:

- Sec. 2009 and Sec. 2010. Increased penalty for improper disclosure or use of information by preparers of returns. The provision would 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. This provision is intended to provide a strong incentive for tax preparers to secure client records, thereby decreasing the likelihood of those records being stolen by criminals.⁸
- Sec. 2202. Limit redisclosures and uses of consent-based disclosures of tax return information. This provision limits tax return information redisclosures by the taxpayer's designee to only those redisclosures to which the taxpayer has expressly consented.⁹
- Sec. 2304. Authentication of users of electronic services accounts. In the past, unscrupulous tax preparers have used the IRS' e-Services to commit tax fraud. The provision requires the IRS to use technical means [such as two-factor or multi-factor authentication (see the definitions chapter)] to verify the identity of any individual

⁶ IRS Publication 1345.

⁷ IRS Publication 1345.

⁸ https://www.finance.senate.gov/imo/media/doc/Taxpayer%20First%20Act_Section%20by%20Section-converted.pdf

⁹ https://www.finance.senate.gov/imo/media/doc/Taxpayer%20First%20Act_Section%20by%20Section-converted.pdf

opening an e-Services account before he or she is able to use such services.^{10, 11}

NOTE: 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. It often involves a security code sent via text.¹²

Predictive Policing

As the IRS increases its information-sharing activities, there may be increased application of artificial intelligence, which may improve identity theft solutions for the detection of taxpayer fraud. The IRS can be expected to use computer data analytics to more frequently identify income tax avoidance and fraud. Don Fort, chief, IRS Criminal Investigation, has stated: “Data analytics and other technologies like ‘predictive policing’ help give law enforcement a clearer picture and are quickly becoming an everyday tool for CI” (IRS Criminal Investigation Annual Report 2018, <http://bit.ly/2LC3Y2>). With this expected increased focus from the IRS, more targeted, predictive examinations should become common practice in the near future.¹³

Cyber Liability Insurance

It is prudent to purchase standalone cyber liability insurance coverage. Cyber liability incidents may be covered under other policies, including Directors and Officers (D&O) and Errors and Omissions (E&O), but practitioners should confirm both the exclusions and limitations of these policies—, as they may be significant. For example, a forensic examination of a single unauthorized release of taxpayer data could result in an expense of several hundred thousand dollars, which may be excluded from D&O and E&O policies.

Also, for any policy in force relating to cyber liability incidents, it is important to read and understand the notification elements required by the policy. For example, the agent/broker/carrier needs to be contacted within a certain number of days after becoming aware of a reportable incident or breach. Because actions or inactions on the practitioner’s part could cause a denial of coverage, review the entire policy at least annually—ideally prior to renewal. Practitioners should also include the exercise of contacting the insurance representative within the practice’s Incident Response Plan (IRP).

Finally, many free sources of cybersecurity information and incentives are available from insurance carriers and brokers.

¹⁰ https://www.finance.senate.gov/imo/media/doc/Taxpayer%20First%20Act_Section%20by%20Section-converted.pdf

¹¹ Top Ten Changes in the Taxpayer First Act of 2019, Sidney Kess, JD, LLM, CPA and Steven I. Hurok, JD, CPA, <https://www.cpajournal.com/2019/09/03/top-ten-changes-in-the-taxpayer-first-act-of-2019/>

¹² “Working Virtually: Use multi-factor authentication to protect accounts; Part 2 of Security Summit tips for tax professionals,” Internal Revenue Service, <https://www.irs.gov/newsroom/working-virtually-use-multi-factor-authentication-to-protect-accounts-part-2-of-security-summit-tips-for-tax-professionals>.

¹³ Top Ten Changes in the Taxpayer First Act of 2019, Sidney Kess, JD, LLM, CPA and Steven I. Hurok, JD, CPA, <https://www.cpajournal.com/2019/09/03/top-ten-changes-in-the-taxpayer-first-act-of-2019/>

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.**”¹⁴ These new publications repeat many of the concepts contained in previous publications and refer practitioners to Publications 4557 and 5293 (which we will explore in detail). One new development in this new series is multifactor authentication for tax software providers (**confirm that your tax software provider is complying with this requirement**):

“NEW” FTC ADOPTS UPDATED SAFEGUARDS RULE¹⁵

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”). This is the first significant update to the FTC’s Safeguards Rule since it took effect in 2003. The Final Rule imposes a number of new specific information security requirements on financial institutions subject to the FTC’s jurisdiction.

Section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 USC 6801(b), requires the FTC and the federal functional financial regulators to ***adopt regulations to establish administrative, technical, and physical security safeguards at financial institutions to protect the security and confidentiality of consumers’ financial information.***

The FTC’s Safeguards Rule implements this GLBA requirement, with the FTC having Safeguards Rule jurisdiction over:

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

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.

In adopting the Safeguards Rule (2003), the FTC sought to provide financial institutions with flexibility in the implementation of their information security programs. In general, under the current version of the Safeguards Rule, financial institutions must conduct a

¹⁴ “Working Virtually: Protecting Tax Data at Home and at Work,” Internal Revenue Service, <https://www.irs.gov/newsroom/working-virtually-protecting-tax-data-at-home-and-at-work>.

¹⁵ <https://www.lexology.com/library/detail.aspx?g=89bb106e-2dd4-43d1-b83a-of2f770c07dc>

risk assessment to identify reasonably foreseeable risks to the security of their customers' information, adopt safeguards to address those identified risks, conduct employee training, and oversee service providers with access to customer information.

The Final Rule maintains the existing Safeguard Rule's basic framework but imposes significant new requirements for financial institutions' information security programs, including:

Appointing a single “qualified individual” to oversee the security program. Although the Final Rule does not define specific qualifications that this individual must possess, the qualified individual must be qualified to oversee and enforce a financial institution's information security program, which will vary based on the size and complexity of the financial institution and its information systems. The Final Rule makes clear that a qualified individual can be an employee, the employee of an affiliate entity, or a service provider.

Conducting a written risk assessment and periodically updating it. In the update, the financial institution must reexamine the evolving risks to its customer information and to information systems that process or have access to such data.

Implementing safeguards to control identified risks. The Final Rule requires specific security measures that financial institutions must implement, including:

1. Technical and physical access controls based on least privilege principles to limit access to customer information.
2. Preparing a system inventory to manage the financial institution's data, information systems, devices, personnel, and facilities so the financial institution can locate customer information and manage systems that may access such information or that are connected to systems that process such information.
3. Encrypting all customer information in transit over external networks and at rest. The FTC declined to limit the encryption requirement to only more sensitive customer information, stating that information revealing that a consumer is a financial institution's customer is itself sensitive. To provide financial institutions with some flexibility, the institution's qualified individual may approve effective alternative compensating controls if encryption is infeasible.
4. Adopting secure development practices for in-house developed software used to transmit, access, or store customer information. Financial institutions also must develop processes to evaluate and test the security of externally developed applications used to process customer information.
5. Implement multifactor authentication for any individual accessing information systems that process customer information, including

customers, employees, service providers, and others. As with encryption, the FTC argues that the security benefits of multifactor authentication outweigh any added financial burdens or inconvenience in a longer log-in process. Again, in an attempt to provide some flexibility, a financial institution's qualified individual may approve (in writing) "reasonably equivalent or more secure access controls."

6. Develop, implement and maintain procedures to securely dispose of customer information. The Final Rule creates a data retention limitation for financial institutions. Under the Final Rule, financial institutions must dispose of customer information no later than two years after the last date the information was used in connection with the provision of a product or service unless the information is necessary for business operations, a legitimate business purpose, is required by law, or disposal is not reasonably feasible.
7. Implement measures to monitor and log the activity of authorized users and detect unauthorized access to customer information.

Regularly testing or otherwise monitoring security controls' effectiveness. Information systems must be continuously monitored or undergo annual penetration testing or biannual vulnerability assessments.

Implementing policies and procedures to ensure personnel are able to meet the information security program's requirements. These include providing security awareness training to employees, utilizing qualified information security personnel, providing information security personnel with training so they are aware of emerging threats and security vulnerabilities, and verifying that information security personnel maintain current knowledge of security threats (to complement the required training).

Periodically assessing service providers' security risks and that the service providers continue to provide the safeguards required by their contract with the financial institution.

Establishing a written incident response plan designed to promptly respond to and recover from security events that materially affect the confidentiality, integrity, or availability of customer information. The "availability" prong is intended to address ransomware and denial-of-service incidents.

Providing annual reports by the qualified individual to the financial institution's board of directors (or equivalent).

The Final Rule includes a limited exception for financial institutions that maintain customer information of fewer than 5,000 persons. The Final Rule takes effect one year after the Final Rule is published in the Federal Register.

Security event notification proposal

In addition to the Final Rule, the FTC initiated a supplemental notice of proposed rulemaking (SNPRM) seeking comment on a proposed Safeguards Rule amendment that would require financial institutions to notify the FTC in the event of a “security event.” The Final Rule defines a “security event” as “an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.”

The proposed amendment would require a financial institution to notify the FTC of a security event affecting at least 1,000 consumers where it is reasonably likely that customer information has been misused. A financial institution would need to notify the FTC within 30 days of discovering the security event.

Comments on the proposed security event notification requirement are due to the FTC within 60 days after the SNPRM is published in the Federal Register.

NOTES

Unit

2

Selected Cybersecurity Terms

LEARNING OBJECTIVE

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Define** key information technology and cybersecurity terms, including encryption and password requirements.

CYBERSECURITY TERMS

The IRS expects tax practitioners to have a basic level of cybersecurity knowledge. We will introduce you to 10 common terms, with definitions and explanations. Next, we'll spend some time getting better acquainted with password best practices and encryption—two items that will immediately strengthen your security if implemented correctly. In fact, encryption can be used as at least a partial defense for breach notification requirements under many states' breach or privacy laws as well as under the European General Data Protection Regulation (GDPR).

While going through the following definitions, keep in mind that the IRS, the FTC, and several state regulators require that you have a written security plan in place that shows you have implemented these items.

CYBERSECURITY

The National Institute of Standards and Technology (NIST), a unit of the U.S. Department of Commerce) defines cybersecurity 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.¹⁶

¹⁶ Small Business Information Security: The Fundamentals (NIST), <https://doi.org/10.6028/NIST.IR.7621r1>

NIST also defines cybersecurity as:

The ability to protect or defend the use of cyberspace from cyberattacks.¹⁷

PRIVACY & CONFIDENTIALITY¹⁸

According to NIST, data privacy is the right of a party to maintain control over and confidentiality of information about itself and “freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.”¹⁹

According to Experian,

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. Ways of securing your data include:

- data encryption—converting the data into a code that cannot be easily read without a decryption key that unlocks it;
- data masking—masking certain areas of data so personnel without the required authorization cannot look at it;
- data erasure—ensuring that no longer used data is completely removed and cannot be recovered by unauthorized people; and
- data backup—creating copies of data so it can be recovered if the original copy is lost.

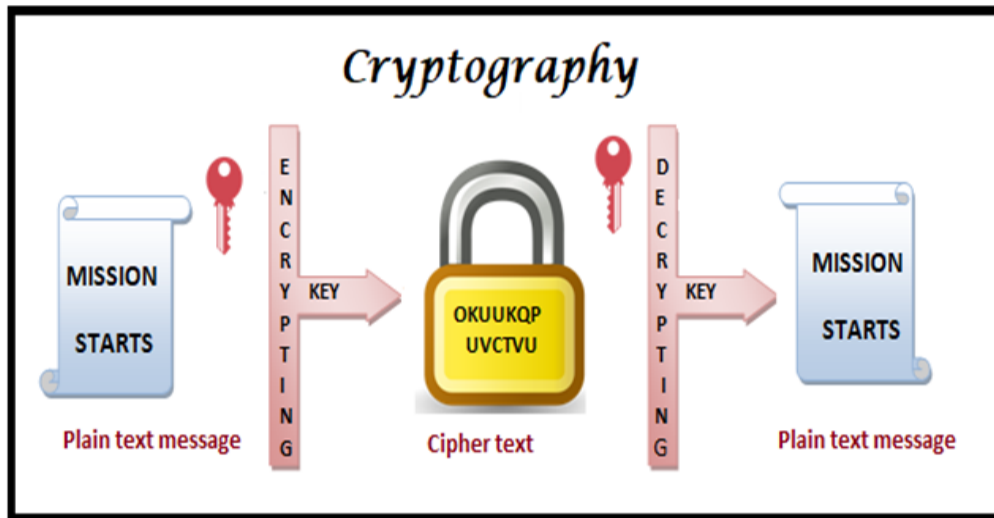
ENCRYPTION

Encryption is rearranging data from plain text (as originally created, what is readable without any additional steps) to **ciphertext**, which is, ideally, a haphazard combination of letters, numbers, and characters that can only be rearranged to the original plain text with a decryption key.

¹⁷ NIST Computer Security Resource Center, <https://csrc.nist.gov/glossary/term/Cyber-Security>

¹⁸ Cybersecurity vs. Data Security, Bruce Sussman, Secureworld, <https://www.secureworldexpo.com/industry-news/cybersecurity-vs-data-security-definition>; <https://www.experian.co.uk/business/glossary/data-security/>

¹⁹ NISTIR 4734 under Privacy; NISTIR 8053 (ISO/IEC 2382).



NIST defines encryption as “the process of changing plaintext into ciphertext.”²⁰

Google Cloud’s definition of encryption follows:

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. The algorithms used in the encryption process are public, but the key required for decrypting the ciphertext is private. Encryption in transit often uses asymmetric key exchange, such as elliptic-curve-based Diffie-Hellman, to establish a shared symmetric key that is used for data encryption.²¹

Google Cloud states that encryption is one piece of a broader security strategy. Encryption adds a layer of defense in depth for protecting data encryption ensures that if the data accidentally falls into an attacker's hands, the attacker will not be able to access the data without also having access to the encryption keys. Even if an attacker obtains the storage devices containing your data, the attacker won't be able to understand or decrypt it.²²

There are three states of encryption: at rest, in transit, and in use. For encryption **at rest**, Google Cloud explains, “protects your data from a system compromise or data exfiltration [unauthorized copying or removing of data] by encrypting data while stored [on a disk or backup media]. The Advanced Encryption Standard (AES) is often used to encrypt data at rest [this is the standard recommended by NIST, preferably at the 256-bit setting].” Encryption at rest reduces the surface of attack by cutting out the lower layers of the hardware and software stack. If these lower layers are compromised (for example, through physical access to devices), the **data** on those devices will not usually be compromised if encryption is deployed. Encryption also acts as a chokepoint;

²⁰ NIST Computer Security Resource Center, <https://csrc.nist.gov/glossary/term/encryption>

²¹ From the Google Cloud Platform Whitepaper Encryption in Transit in Google Cloud, last updated November 7, 2019, <https://cloud.google.com/security/encryption-in-transit/>

²² From the Google Cloud Platform Whitepaper Encryption in Transit in Google Cloud, last updated November 7, 2019, <https://cloud.google.com/security/encryption-in-transit/>

centrally managed encryption keys create a single place where access to data is enforced and can be audited.²³

Encryption **in transit**, according to Google Cloud, “protects your data if communications are intercepted while data moves between your site and the cloud provider or between two services. This protection is enabled by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival. For example, Transport Layer Security (TLS) is often used to encrypt data in transit for transport security, and Secure/Multipurpose Internet Mail Extensions (S/MIME) is used often for email message security.”²⁴

Finally, Google Cloud describes encryption in use as encryption that “protects your data when it is being used by servers to run computations.”²⁵

Use Encryption for Sensitive Business Information

According to NIST, “Encryption is a process of making your electronically stored information unreadable to anyone not having the correct password or key.” NIST advises using “full-disk encryption—which encrypts all information on the storage media—on all of your computers, tablets, and smartphones. Many systems come with full-disk encryption capabilities. Not all mobile devices provide this capability,” so practitioners should check to confirm whether this is the case.²⁶

“Do not forget your encryption password or key!” NIST warns that “if you lose or forget your password or 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.” Keep track of its location, and ensure that access is restricted.²⁷

When you send sensitive taxpayer-related documents or emails, “you may want to consider encrypting those documents and/or emails. Many document and email applications provide for this capability.”²⁸

According to NIST, “Typically, the receiver will need to have the same application to decrypt the message or document as you used to encrypt it. If you need to send them a password or key, give it to them via phone or other method. Never send it in the same email as the encrypted document [better yet, make a call to reveal the key—this is known as an out of band communication, which is transmitted in a different mode than the original communication was made known].”

²³ From the Google Cloud Platform Whitepaper Encryption in Transit in Google Cloud, Last updated November 7, 2019, <https://cloud.google.com/security/encryption-at-rest/>

²⁴ From the Google Cloud Platform Whitepaper Encryption in Transit in Google Cloud, Last updated November 7, 2019, <https://cloud.google.com/security/encryption-in-transit/>

²⁵ From the Google Cloud Platform Whitepaper Encryption in Transit in Google Cloud, Last updated November 7, 2019, <https://cloud.google.com/security/encryption-in-use/>

²⁶ NISTIR 7621-Revision 1 Small Business Information Security.

²⁷ NISTIR 7621-Revision 1 Small Business Information Security.

²⁸ NISTIR 7621-Revision 1 Small Business Information Security, p. 21.

Google Cloud suggests that practitioners use encryption as “one component of a broader security strategy. Encryption in transit defends your data, after a connection is established and authenticated, against potential attackers by removing the need to trust the lower layers of the network which are commonly provided by third parties; reducing the potential attack surface; and, preventing attackers from accessing data if communications are intercepted.”²⁹

Encryption may act as at least a partial defense in a reportable breach situation under most privacy and security regulations if the encryption key or password has not been lost or stolen. Practitioners should confirm with legal counsel and/or their insurance liability carrier(s).

Should practitioners encrypt data or the device, or both? Device/hardware encryption may be better, but look at the default settings and make sure they are up to date and configured in line with guidance from your device’s operating system manufacturer—even with these safeguards, your data may still be at risk if there is an undiscovered settings error.³⁰

In one instance, a well-known software encryption solution (BitLocker), when enabled, “trusted” (took no action) for encrypting an SSD laptop hard drive (solid-state hard drive—no moving parts), under default settings, because it recognized that a hardware encryption solution had already been installed on the hard drive by the manufacturer.

BitLocker did not recognize that the laptop’s hard drive encryption solution was faulty, so there was **no encryption at all** for data on this laptop.³¹ Unfortunately a large number of laptops were affected by this defect, but a solution was eventually crafted by BitLocker’s owner, Microsoft.³²

Moral of this story: although this is an extreme case and in reality a hardware issue, the best plan is to always check your default settings, especially for encryption. Also, always check for updates and bulletins published by your operating system (OS) and encryption vendors.

ENCRYPTION: IMPLEMENTING ENCRYPTION SYSTEMS AVAILABLE FOR COMPUTERS, SMARTPHONES & TABLETS

Encryption for email should be TLS version 1.2 or 1.3 /256 –bit AES encryption (at rest), at a minimum, for sensitive email.

Your email archive should also be encrypted with limited access. As always, confirm that encryption keys and all passwords that lead to locations with sensitive/confidential data

²⁹ From the Google Cloud Platform Whitepaper Encryption in Transit in Google Cloud, last updated November 7, 2019, <https://cloud.google.com/security/encryption-in-transit/>

³⁰ Hardware Encryption vs. Software Encryption: The Simple Guide, September 12 2017, Sam Wiltshire, <https://www.ontrack.com/blog/2017/09/12/hardware-encryption-software-encryption/>

³¹ You Can’t Trust BitLocker to Encrypt Your SSD on Windows 10, How to Geek.com, Chris Hoffman, Updated September 27, 2019, <https://www.howtogeek.com/fyi/you-cant-trust-bitlocker-to-encrypt-your-ssd-on-windows-10/>

³² ADV180028 | Guidance for configuring BitLocker to enforce software encryption, Security Advisory, Published: 11/06/2018, <https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/ADV180028>

meet complexity, non-sharing, and longevity requirements (see details in separate password section).

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 bring your own device (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 inventory of all BYOD devices as well as those that are firm-issued in order to allow the MDM solution to be effective.³³

Additional Mobile Device Recommendations

When taking inventory of mobile devices, don't forget to inventory the applications that sync to these mobile devices, including smart watches and other wearables. If BYOD is limited to email only, encryption can be applied to the email and email archive, with multi-factor authentication (MFA) on the devices used as an added security tool.

Monitoring is critical when a mobile device has been lost or stolen—the administrator should be able to remotely lock the device when a monitoring alert has been received and after the employee reports the loss. In general, the MDM solution should allow the administrator to remotely wipe the device (but ensure that the employee's non-work data is not wiped; apart from angering your employee, practitioners may be violating a state privacy law and/or the GDPR).

In general, your administrator will be able to remotely locate the device when reported lost or stolen, but again, confirm that your monitoring actions do not violate a privacy law—confirm with counsel.

During normal employee use, copy/paste of firm documents and camera use can be blocked, and permissions can be applied for, when using firm-issued devices. These actions reduce the chance of lost/stolen data under data loss prevention (DLP) best practices. MDM can also push out operating system (OS) and third-party software/application updates to mobile devices. Finally, MDM solutions can be set to whitelist (accept) or blacklist (reject) applications based on a number of criteria set by the administrator.³⁴

³³ NISTIR 7621-Revision 1 Small Business Information Security.

³⁴ NISTIR 7621-Revision 1 Small Business Information Security.

Additional Encryption Links

Detailed encryption information for Microsoft O365, including SharePoint and OneDrive:

- Data Encryption in OneDrive for Business and SharePoint Online (Data in Transit), <https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-for-data-in-transit>
- Data Encryption in OneDrive for Business and SharePoint Online (Data at Rest), <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo#encryption-of-data-at-rest>

Basic information on how to protect files, through a password or encryption:

- Protect an Excel file, <https://support.office.com/en-us/article/protect-an-excel-file-7359d4ae-7213-4ac2-b058-f75e9311b599>
- How to encrypt a file (Applies to: Windows 10), <https://support.microsoft.com/en-us/help/4026312/windows-10-how-to-encrypt-a-file>

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. Sometimes the bad actor will delete your data even after receiving the ransomware funds. The bad actor usually gains access to your data through your network/webpage/app/portal or through your vendor/subvendor's versions of these.

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/password is located.

Vendor oversight is extremely important in reducing the likelihood of becoming a ransomware victim. Ensure that your vendors have cybersecurity controls in place and confirm with counsel [a good place for this is in the terms of your vendor contract or service-level agreement (SLA)].

PASSWORDS

The IRS and NIST both require an 8-character minimum (best IT practices suggest a 12-character minimum). Passphrases are better than passwords, and the key concepts for passwords or passphrases are length and complexity.³⁵

Do not reuse the same password (using the same password for multiple purposes especially for financial logins). If a hacker accesses the password from one source, the

³⁵ <https://www.irs.gov/newsroom/national-tax-security-awareness-week-day-3-creating-strong-passwords-can-protect-taxpayers-from-identity-theft>

hacker will continue and possibly clean out your bank account(s)! Create unique passwords for every website and app.³⁶

Change or refresh your passwords at regular intervals, especially for financial logins!^{37, 38}



Source: <https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5word>

Worst Passwords of 2021 from NordPass³⁹

Do not use these passwords!

Worst Passwords of 2020 from NordPass

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

³⁶ <https://www.irs.gov/newsroom/national-tax-security-awareness-week-day-3-creating-strong-passwords-can-protect-taxpayers-from-identity-theft>

³⁷ <https://www.irs.gov/newsroom/national-tax-security-awareness-week-day-3-creating-strong-passwords-can-protect-taxpayers-from-identity-theft>

³⁸ Hacked Dropbox login data of 68 million users is now for sale on the dark Web, Karen Turner, September 2016, <https://www.washingtonpost.com/news/the-switch/wp/2016/09/07/hacked-dropbox-data-of-68-million-users-is-now-or-sale-on-the-dark-web/>

³⁹ "Most common passwords of 2020," NordPass, <https://nordpass.com/most-common-passwords-list/>.

Password Managers

Password managers are good tools to manage all of your passwords. PC Magazine has ranked what it considers to be the best for 2020 at The Best Password Managers for 2020, 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 (for example, the IRS requires a minimum of eight characters) or the requirements of a specific webpage or app.
- 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.”⁴⁰
- 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.”⁴¹
- 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.”⁴²

Most password manager credentials are in a database protected with AES-256 encryption. To unlock the password database, the user enters a decryption key (user's master password) known only to the user.

In addition, password managers that sync your password database to the cloud use end-to-end encryption. The data is encrypted before it leaves the user's device, and it stays encrypted as it's transferred to the remote server. When the user signs in to the app on a local device, “the program sends a one-way hash of the password that identifies the user but can't be used to unlock the file itself.”

Also, the companies that manage and sync those saved files don't have access to the decryption keys- the master password isn't stored anywhere, and if the user forgets it, there is no way to access the user's data. “There's no known way to crack an AES-256 encrypted file that's protected with a strong personal key.”⁴³

⁴⁰ 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/>

⁴¹ 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/>

⁴² 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/>

⁴³ 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/>

REPORTABLE BREACH/SECURITY 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.⁴⁴

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.⁴⁵

MULTI-FACTOR AUTHENTICATION

NOTE: Since 2021, all tax software providers have been required to offer multi-factor authentication options on their products that meet higher standards. A multi-factor or two-factor authentication offers an extra layer of protection for the username and password used by the tax professional. It often involves a security code sent via text.⁴⁶

Multi-factor authentication (MFA) is generally a few pieces of information (“factors”) which include at least the following: what you have, what you know, and what you are. MFA is more secure than two-factor authentication (which is generally only a user ID and a password).

According to a New York State Regulatory body, multi-factor authentication means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, (what you know) such as a password; or (2) possession factors, such as a token or text message on a mobile phone (what you have); or (3) inherence factors, such as a biometric characteristic (what you are).⁴⁷

PERSONALLY IDENTIFIABLE DATA/TAXPAYER DATA

IRS/IRC definition: Taxpayer data is “defined for our purposes as personally identifiable information and other personal, financial, or federal tax data.”⁴⁸

IRS definition of tax return information: Tax return information is 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. 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 tax return preparation software

⁴⁴ GAO-19-340 Taxpayer Information.

⁴⁵ Pub 1345, p. 7.

⁴⁶ “Working Virtually: Use multi-factor authentication to protect accounts; Part 2 of Security Summit tips for tax professionals,” Internal Revenue Service, <https://www.irs.gov/newsroom/working-virtually-use-multi-factor-authentication-to-protect-accounts-part-2-of-security-summit-tips-for-tax-professionals>.

⁴⁷ 23 NYCCR Section 500.01, NYDFS (New York State Department of Financial Services) Cybersecurity Regulation.

⁴⁸ NYDFS Cybersecurity Regulation, Section 500.01, Definitions.

registration information. All tax return information is protected by Section 7216 and the regulations.⁴⁹

State definitions include name, email social security number, address, passport number, IP address, ID/password.

Gramm-Leach-Bliley Act (GLBA) definition: “Nonpublic personal information” is defined as personally identifiable financial information and 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. 16 CFR 313.3(n) (1). The Safeguards Rule uses the definition of “nonpublic personal information” from the Privacy Rule. The Safeguards Rule uses the definitions of “customer” and “customer relationship” from the Privacy Rule.⁵⁰

NIST: Personal information includes “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.”⁵¹

ANTIVIRUS

Antivirus software is used to protect computers and or devices from getting infected with **malware**. The antivirus software runs in the background scanning downloads, attachments, and files. When an infection is detected, the antivirus software will/should notify the user and move into quarantine folder to prevent/stop further infection.⁵²

11 Infections Malware Types to Watch Out for in 2021⁵³

1. Ransomware

Ransomware is a type of software that uses encryption to block a computer user or owner from accessing their data until a ransom gets paid. This software keeps the victim, whether a person or a company, from being able to operate until that money gets sent to the perpetrator.

Unfortunately, even if you pay the ransom there is no guarantee that they'll allow you access to your data again.

2. Fileless Malware

Fileless malware works in a very similar fashion to a trojan virus or computer worm. It doesn't install any software onto your computer. Instead, it makes changes to native

⁴⁹ <https://www.irs.gov/tax-professionals/section-7216-frequently-asked-questions>; IRC Section 7216 (Page Last Reviewed or Updated: 15-Jul-2020).

⁵⁰ GLBA/FTC: 16 CFR 314.2(b), 16 CFR 616 CFR 313.3(h), (i), 16 CFR 314.2(a).

⁵¹ NISTIR 7621-Revision 1 Small Business Information Security, p. 5.

⁵² <https://www.irs.gov/privacy-disclosure/computer-virus-technical-assistance>

⁵³ <https://www.crtucson.com/11-infectious-malware-types-to-watch-out-for-in-2021/>

operating system files. This tricks your computer into thinking the changes are legitimate.

If you have an antivirus program, fileless malware can slip past it since it makes small changes to files that belong on your computer. Due to the stealth of these attacks, they are much more successful than other types of viruses.

3. Spyware

Spyware does exactly what its name implies. It collects information about a user's activity stealthily. It works without the user even knowing that it is collecting all of their data and information.

This information includes usernames, passwords, PINs, and even payment information. Spyware isn't exclusive to just desktop computers, either. It is also a threat on mobile devices that you need to take seriously.

4. Adware

Similar to spyware, adware tracks a user's web browsing activities and decides which ads should get served to you based on that data. Adware is similar to fileless malware because it doesn't install anything on your computer.

The biggest threat of adware is the continued erosion of your privacy. This data gets collected and used to build a profile about you. It is then sold to marketers for them to market their products to you without your consent.

5. Trojan

A trojan virus is tricky because it disguises itself as a desirable type of software but once it has been downloaded it takes control of your systems.

The most common places for trojans to hide are in games and apps. Some have even been found in fake patches for software.

6. Worms

Worms work by targeting vulnerable parts of your operating systems. They install themselves into your networks and find access through multiple points. They'll find backdoors into software and other parts of your computer.

The most common reasons for the use of worms are to steal sensitive data that belongs to you, as well as to attempt ransomware attacks.

7. Virus

A computer virus is a simple piece of computer code that finds a way into an application on your computer. Once that app is accessed the code executes its function.

Viruses are primarily used to steal sensitive information as well as to launch ransomware attacks on the user. They are completely dependent on a host file or host application in order to be effective.

While viruses may seem similar to trojans, they can't work or reproduce unless the app they're hiding in is run. Trojans work by requiring the user to download them and grant them access to their data and information. If you need a virus removed from your computer this is the perfect place to get help.

8. Rootkits

Rootkits are one of the scariest malware types because it gives the malicious actor remote access and control of your computer with full capabilities. Rootkits are found in applications, kernels, and firmware.

The most common way for rootkits to spread is through phishing emails and malicious attachments as well as malicious downloads. On top of that, Rootkits can conceal other types of malware within them.

9. Keyloggers

This type of spyware works by monitoring your activity on your computer. Keyloggers have a legitimate use for monitoring employee activity at a corporation.

They can also be used with malicious intent. They are commonly used to steal sensitive data like your passwords and your banking or payment information. Keyloggers get inserted into a computer through phishing, attachments, as well as social engineering.

10. Botnets

Bots are automated applications that are built to perform tasks on your computer. Like keyloggers, they have a legitimate use but malicious actors have turned them into something more sinister.

Bots have the ability to connect to a central server and form a network as a means of coordinating flood attacks. These attacks have involved over two million computers in the past and are capable of expanding quickly.

11. Mobile Malware

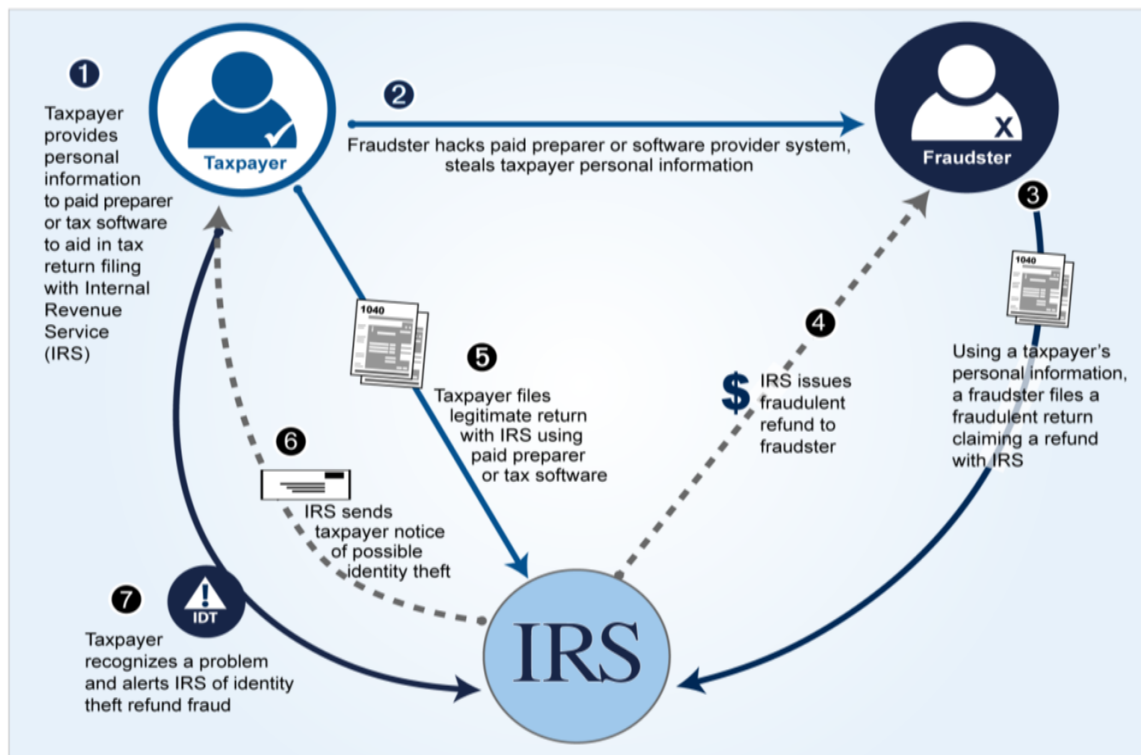
Malware has made an increased effort to target mobile devices in recent years, with 2019 seeing a 50 percent increase in mobile malware attacks. Mobile malware comes in all different shapes and forms.

Common types of mobile malware are trojans and ransomware and they come as a result of malicious downloads and phishing. They are especially troublesome for smartphones that are jailbroken since they're no longer protected by the phone's operating system protection software.

TAXPAYER FRAUD

Tax fraud is defined as personally identifiable information and other personal, financial, or federal tax data—which can then be used to commit identity theft refund fraud or other types of financial crimes. Viewed broadly, identity theft 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. Figure 1 presents an example of how this crime can work. In this example, a taxpayer may alert the IRS of identity theft refund fraud. Alternatively, the IRS can detect identity theft refund fraud through its automated filters that search for specific characteristics, as well as through other reviews of taxpayer returns.⁵⁴



Source: GAO analysis. | GAO-19-340

Source: GAO-19-340 Taxpayer Information flow

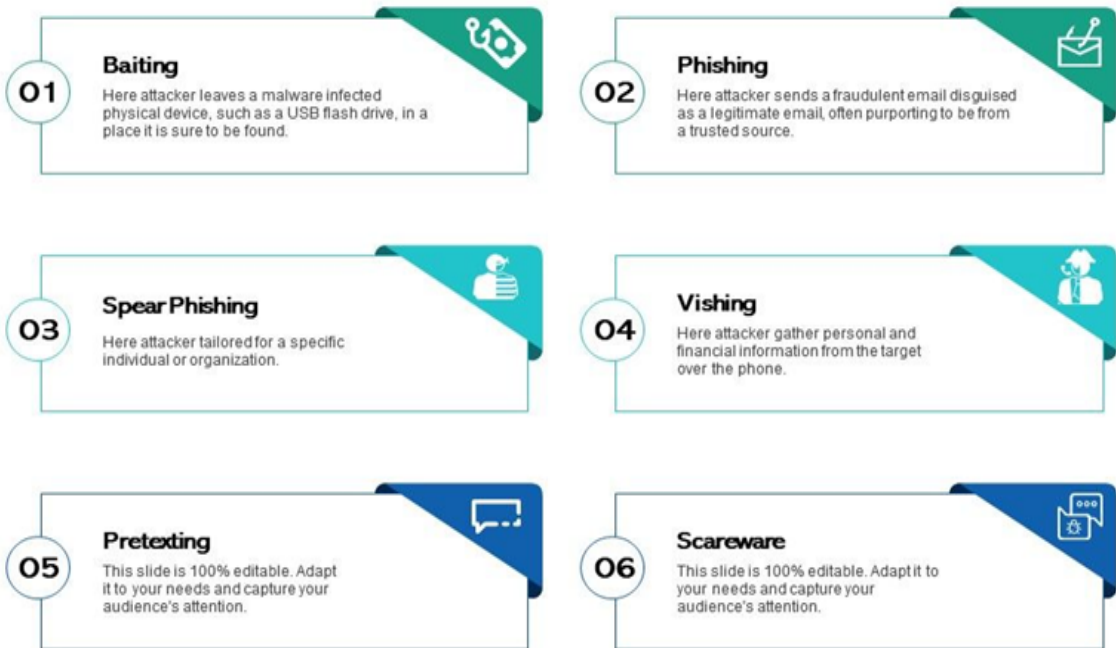
SOCIAL ENGINEERING

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. There are a number of ways social engineering attacks are carried out:⁵⁵

⁵⁴ GAO-19-340 Taxpayer Information.

⁵⁵ <https://www.us-cert.gov/ncas/tips/ST04-014>

6 Types of Social Engineering Attack



Source: <https://www.slideteam.net/6-types-of-social-engineering-attack.html>

Phishing

What is a phishing attack?

According to Imperva, a well-known IT security provider, 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.⁵⁶

Imperva states that phishing is often used to gain a foothold in corporate or governmental 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.⁵⁷

⁵⁶ Phishing attacks, October, 2019, <https://www.imperva.com/learn/application-security/phishing-attack-scam/>

⁵⁷ Phishing attacks, October, 2019, <https://www.imperva.com/learn/application-security/phishing-attack-scam/>

Finally, Imperva warns that an organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.⁵⁸

The first known phishing attack was identified in 1996 on an AOL account.⁵⁹

Phishing attacks use email or fake websites, which appear to be legitimate, to trick users into giving up their personal data. For example, an attacker may send email from what looks to be a reputable credit card company that requests account information “because there is a problem with your account” or even better, “because your account has just been hacked.” There is always a sense of urgency in phishing attacks. When users respond with the requested information, attackers can use it to gain access to the accounts.

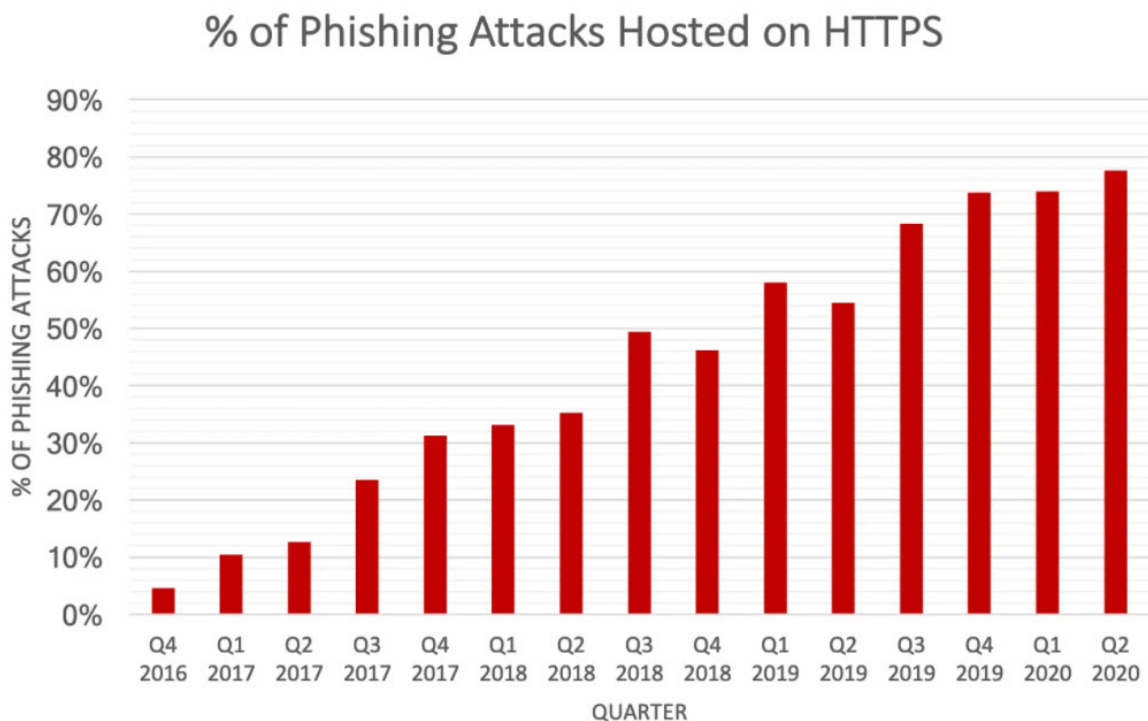
Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami),
- epidemics and health scares (e.g., COVID-19),
- economic concerns (e.g., IRS scams),
- major political elections,
- major sports events, and
- holidays.⁶⁰

⁵⁸ Phishing attacks, October, 2019, <https://www.imperva.com/learn/application-security/phishing-attack-scam/>

⁵⁹ <https://www.malwarebytes.com/phishing/>

⁶⁰ <https://www.us-cert.gov/ncas/tips/ST04-014>



Source: <https://digitalguardian.com/blog/phishing-bec-scams-netting-80000-average-2020>

Don't click the link!

Common phishing attacks & how to protect against them

According to the FTC, email phishing is a numbers game. An attacker who sends 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.

In addition, attackers design phishing messages to mimic actual emails from a spoofed organization by using the same phrasing, typefaces, logos, and signatures to make the messages appear legitimate.

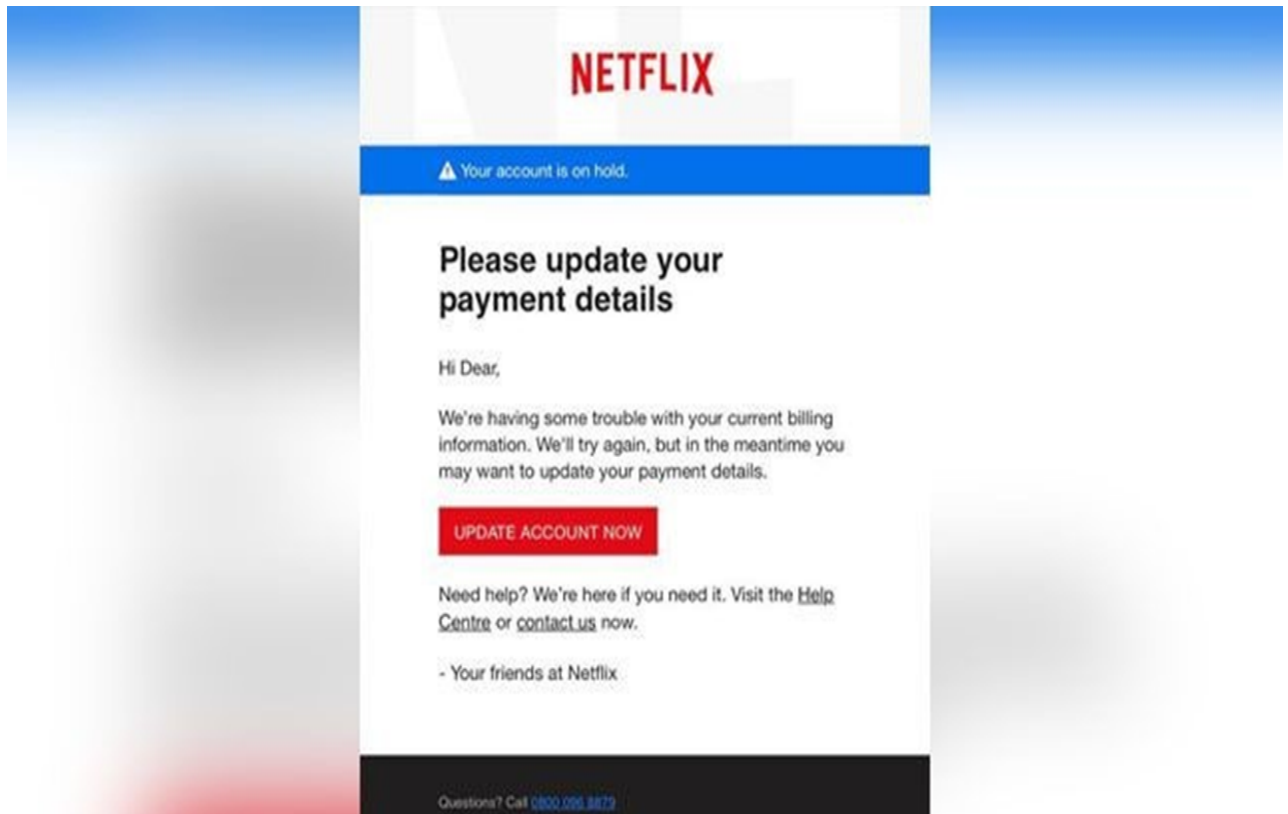
Also, attackers will usually try to push users into action by creating a sense of urgency. For example, an email could threaten account expiration and place the recipient on a timer. Applying pressure causes the user to be less prudent and more prone to error.

Moreover, links inside messages resemble their legitimate counterparts but typically have a misspelled domain name or extra subdomains. For example, **“myuniversity.edu/renewal”** can be changed to **“myuniversity.edurenewal.com.”**

Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.⁶¹

⁶¹ How to Recognize and Avoid Phishing Scams, <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

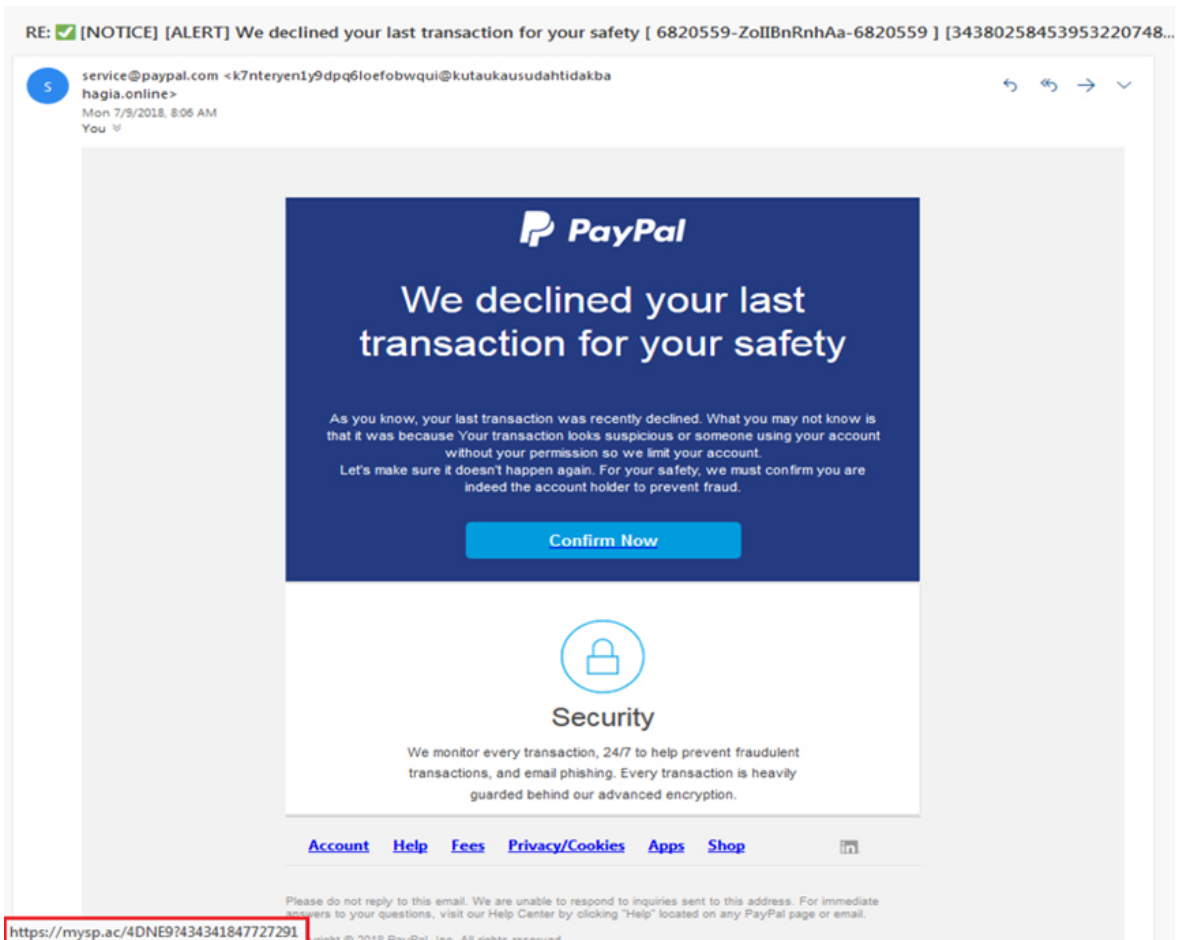
The following pages show three examples of phishing attacks.



Source: How to Recognize and Avoid Phishing Scams,
<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

Comments: “Hi Dear” (!)—Notice the urgent “Update Account Now” wording in an attention-getting red rectangle.

Except for the salutation, the grammar and spelling are not bad here.



Source: <https://www.malwarebytes.com/phishing>

Comments: Note the urgent “Confirm Now” button. Moving your mouse over this button reveals the actual URL destination (in the red-outlined rectangle), which—has nothing to do with PayPal.



Amazon Inc. <noreply@Amz-ID-boFmQ2R3J8PPJ.com>
Fri 7/20/2018, 1:44 AM
You

Dear Customer ,

ID:XQ6XE6SYJSGUJS

We detected suspicious activity in your account and multiple password used for access your account.

We need you to confirm your account !

1. [Click Here](#) to confirm your account.
2. Enter your informations.
3. Finally your account will be confirmed.

Note : If you don't confirm it within 48 hours, we will close or suspend your account.

Sincerely,
Amazon.

<https://taadod.biz/8C67A1974/r/eS2MNLmC2=.mFb4EAoZkyCCS>

Source: <https://www.malwarebytes.com/phishing>

Comments: This one is from “Amazon Inc.” “Note: if you don’t respond within 48 hours, we will...” Again, notice the sense of urgency here as well as the actual email address and URL.

Business Email Compromise

According to Help Net Security, an online IT e-zine, business email compromise (BEC) scams remain highly damaging. These attacks target employees who have access to company finances or valued data assets, usually by sending them email from fake or compromised email accounts (a spear phishing attack). 40 percent of BEC attacks use a domain name registered by a scammer. These domains are often slight variations of a trusted, existing company name, meant to fool unwary victims.

Vishing, Deep Fakes, Spear Phishing & Smishing

What is a vishing attack?

Vishing is a voice-based social engineering attack that can be combined with other forms of social engineering to trick a victim into calling a phone number and then verbally revealing personal data.

According to the U.S. Department of Homeland Security’s CISA Cyber Unit, 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.⁶²

A vishing attack: deep fakes

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (\$243,000) 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 artificial intelligence (AI) experts have predicted that criminals would use AI to automate cyberattacks.⁶³

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's slight German accent and the melody of his voice on the phone. It appears that attackers have started to use publicly available voice recordings (commonly found in social media, including on LinkedIn) to impersonate celebrities or executives.⁶⁴

Research is ongoing to study deep fake video, which takes this type of cybercrime to another AI level. The U.N. Center on AI and Robotics at the United Nations Interregional Crime and Justice Research Institute is researching technologies to detect fake videos, which could be an even more useful tool for hackers.⁶⁵

What is a spear phishing attack?

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

Here are four spear phishing examples (from Imperva):

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.

⁶² Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks, Last revised: August 22, 2019, Cybersecurity and Infrastructure Security Agency (CISA), <https://www.us-cert.gov/ncas/tips/ST04-014>

⁶³ <https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/>

⁶⁴ <https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/>

⁶⁵ Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, By Catherine Stupp, Updated Aug. 30, 2019, The Wall Street Journal, <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

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.⁶⁶

What is a smishing attack?

According to the Department of Homeland Security’s CISA Cyber Unit, **smishing** is a type of social engineering that exploits text messages (SMS).

Text messages generally contain links to 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.⁶⁷

How to protect yourself from phishing attacks

The U.S. Department of Homeland Security (DHS) recommends to ensure that your email spam filters are on so that phishing emails are kept to a minimum. DHS also recommends that businesses be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. DHS also advises that businesses take the following precautions:⁶⁸

- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information—call to confirm.
- Don’t reveal personal or financial information in email, and do not respond to email solicitations for this information, ever! This includes following links sent in email.
- Don't send sensitive information over the internet before checking a website's security and/or calling.
- Minimize publishing sensitive firm details and information on social media (LinkedIn, Facebook, the corporate website). Think before you post!
- 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 slight variation in spelling or a different domain (e.g., .com vs. .net) as seen the above example.

⁶⁶ <https://www.imperva.com/learn/application-security/phishing-attack-scam>

⁶⁷ Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks, Last revised: August 25, 2020, Cybersecurity and Infrastructure Security Agency (CISA), <https://www.us-cert.gov/ncas/tips/ST04-014>

⁶⁸ Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks, Last revised: August 25, 2020, Cybersecurity and Infrastructure Security Agency (CISA), <https://www.us-cert.gov/ncas/tips/ST04-014>

- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly (calling is the best way to confirm). Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (APWG). You can browse the APWG's eCrime Research Papers for examples.
- Install and maintain antivirus software, firewalls, and email filters (e.g., DMARC) to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Never store passwords in your browser.
- Enforce multi-factor authentication.
- Require social awareness training 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.⁶⁹

⁶⁹ Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks, Last revised: August 25, 2020, Cybersecurity and Infrastructure Security Agency (CISA), <https://www.us-cert.gov/ncas/tips/ST04-014>

NOTES

Unit

3

IRS Guidance & Regulations Relating to Cybersecurity & Protecting Taxpayer Data

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Explore** the basic taxpayer data protection requirements mandated by several IRS publications.
- ☐ **Outline** the key privacy and security issues a tax practitioner must be aware of when processing or handling taxpayer data.
- ☐ **Explain** to your clients the protections that you are using to secure their data.
- ☐ **Apply** the required cybersecurity protections to your taxpayer data.

As we discussed initially, the IRS requires a baseline for protection of taxpayer data—**this is considered the bare minimum for compliance**. Several IRS publications describe this baseline in detail—4557, 1345, 5293, and IR-2019-127. We'll start with Publication 4557.

IRS PUBLICATIONS

IRS Publication 4557, Safeguarding Taxpayer Data: A Guide for Your Business

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

Publication 4557's 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. It is essential to have a set of formal written controls over the most important areas of your taxpayer client data protection program. Many of these controls involve a monitoring function.

We'll unpack this publication, section by section, starting with the Review Internal Controls section.

Review Internal Controls

There are generally three components to most day-to-day governance: policies, procedures, and controls. Policies are high-level statements (e.g., the acceptable use policy (AUP)). Procedures are detailed and granular instructions on how to make the policy statements work:

1. An admin with admin credentials (administrator access privileges) to the network activity log will on a weekly basis use the firm's network admin password to access logs of internet activity.
2. The admin will examine the access logs and will report activity which our security software has flagged for violations of the acceptable use policy.

Controls are the means for getting the procedures completed, as well as to provide evidence that procedures have been performed. In our example, a control for enforcement of the acceptable use policy could be a progressive disciplinary action for employees who are found to have violated the policy, blacklisting (blocking) all prohibited sites, or ensuring that metadata evidence showing admin manual review of log data is collected and retained.

Publication 4557 requires that the following controls are formalized and implemented—you may need to show the IRS evidence that these controls are in place:⁷⁰

- Install anti-malware/antivirus security software on all devices (laptops, desktops, routers, tablets, and phones) and keep software set to automatically update; use strong passwords of eight or more characters, use different passwords for each account, use special and alphanumeric characters, use phrases, password protect wireless devices and consider a password manager program—best practices suggest a 14-character password and using a password manager or password vault.⁷¹
- 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 tax return information—especially direct deposit information—prior to e-filing; wipe or destroy old computer hard drives and printers that contain sensitive data.
- Ensure that you follow all applicable data disposal laws.

⁷⁰ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁷¹ <https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines>

- Limit access to taxpayer data to individuals who need to know.
- Check IRS e-Services account weekly for number of returns filed with your EFIN.
- Withdraw from any outstanding authorizations (power of attorney/tax information) for taxpayers who no longer are clients.

Use Security Software

It is imperative in today's cybersecurity environment that you install and update your security software. In addition to the Publication 4557 list below, consider adding a mobile device management (MDM) solution for all firm-issued and employee-owned devices (BYOD) to ensure that all mobile devices are at the same level of security as desktops and workstations. Note the brief Publication 4557 definitions after the security solution names:⁷²

- **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—. Firewalls can exist as software or a hardware device. Next generation firewalls include incident detection systems/incident prevention systems; **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. Download security software only from the chosen vendor's site.⁷³

Create Strong Passwords

We visited passwords in a previous section, but the IRS-specific requirements are good to know, including that all tax practitioners must establish strong, unique passwords for all accounts, whether to access a device, tax software products, cloud storage, wireless networks, or encryption technology:⁷⁴

- Use a minimum of eight to nine characters; longer is better—best practices encourage fourteen characters; more complexity results in better security—use a combination of letters, numbers and symbols (i.e., ABC, 123, !@#).
- Avoid personal information or common passwords/passphrases (for example, “mary/james bond had a little lamb 007%”) are more secure; change default/temporary passwords that come with accounts or devices, including printers.

⁷² IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁷³ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁷⁴ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

- 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—you may want to use a password manager or password vault instead of a paper list. Do not share or disclose your passwords to anyone for any reason—if your bank or credit card company requests your password or pin number, especially by email, confirm that the request is genuine by either calling or going to a branch—the request is usually an attempt at social engineering, as discussed earlier.
- Use a password manager program to create, track, and manage passwords, but protect it with a strong password/passphrase—don't forget this passphrase, because if you do, you will be locked out of your password manager/vault!
- Use multi-factor authentication (MFA) wherever possible.

Secure Wireless Networks

Many common attacks are launched on wireless networks, so the IRS reminds tax practitioners to take the following common-sense precautions. When accessing a public network, only go in through a virtual private network (VPN) and resist the urge to click in directly in the library or at your local coffee shop. According to the IRS, failing to protect your wireless network makes the network or data vulnerable to attack or interception by cybercriminals. Thieves could be stealing your data without your knowledge. You can take these protective steps with setting up your router or review your router's manual to make changes. Here are basic steps to protect your wireless network:⁷⁵

- Change the 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 (i.e., BobsTaxService), and disable the SSID broadcast so that it cannot be seen by those who have no need to use your network.
- Use Wi-Fi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption—AES 256 bit is the optimum setting.
- Do not use Wired-Equivalent Privacy (WEP) to connect your computers to the router; WEP is not considered secure.
- Do not use public Wi-Fi (for example, at a coffee café or airport) to access business email or sensitive documents—but, if firm employees must occasionally connect to

⁷⁵ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide for Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

unknown networks or work from home, establish an encrypted Virtual Private Network (VPN) to allow for a more secure connection. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. Search for “Best VPNs” to find a legitimate vendor; major technology sites often provide lists of top services.⁷⁶

Protect Stored Client Data

The main goal of this course and the IRS’s cybersecurity requirements are the same—to protect taxpayer client data from unauthorized access. The IRS states that Cybercriminals work hard through various tactics to penetrate your network or trick you into disclosing passwords. They may steal the data, hold the data for ransom, or use your own computers to complete and file fraudulent tax returns. Here are a few basic steps to protect client data stored on your systems:⁷⁷

- Use drive encryption to lock files and all devices. Encrypted files require a password to open. Therefore, if an encrypted mobile device is lost or stolen, it will be very difficult for a bad actor to access data stored on the device. Backup encrypted copies of client data to external hard drives (USBs, CDs, and DVDs) or use cloud storage. Keep external drives in a secure location. Encrypt data before uploading to the cloud—you, not the cloud provider, are responsible for securing your data before it gets to the cloud.
- Avoid attaching USB drives and external drives with client data on them to public computers. Set a policy and lock down your firm-issued devices so that USB ports are made inoperable.
- Avoid installing unnecessary software or applications to the business network. Avoid free software, especially security software, which is often a ruse by criminals; download software or applications only from official sites.
- Perform an inventory of devices where client tax data are stored, such as laptops, smartphones, tablets, external hard drives, etc. Inventory software used to process or send tax data, including operating systems, browsers, applications, tax software, websites, etc. You are required to know where client data is stored.
- 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. Some security software include a shredder that electronically destroys stored files. It is also important to know your applicable state data disposal laws as well.
- 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.

⁷⁶ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁷⁷ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

Spot Data Theft

The next two subsections of Publication 4557 relate to monitoring requirements that tax practitioners must perform—the second monitoring section relating to PTINs is limited to CPAs, attorneys, enrolled agents, or Annual Filing Season Program participants and who file 50 or more returns.

Practitioners should establish a routine of carrying out these steps on a weekly basis—the IRS expects you to be doing this.

The IRS identifies these items as common clues to data theft that you should be know:⁷⁸

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

Monitor EFINs/PTINs

The IRS expects practitioners to monitor your Electronic Filing Identification Number (EFIN), Preparer Tax Identification Number (PTIN), and Centralized Authorization File (CAF) activity.

The IRS states that practitioners can obtain a weekly report of the number of tax returns filed with your EFIN or your PTIN. Only those preparers who are attorneys, CPAs, enrolled agents or Annual Filing Season Program participants and who file 50 or more returns may obtain PTIN information. Weekly checks will help flag any abuses.⁷⁹

⁷⁸ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁷⁹ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

For EFIN totals:

- access your e-Services account and your EFIN application;
- select “EFIN Status” from the application; and
- contact the IRS e-help Desk if the return totals exceed the number of returns you filed.
- Deactivate unused EFINs to avoid potential abuse/misuse.

For PTIN totals:

- access your online PTIN account;
- select “View Returns Filed Per PTIN”; and
- complete Form 14157, Complaint: Tax Return Preparer, to report excessive use or misuse of PTIN.

Finally, if you have a CAF number, make sure you keep your authorizations up to date. Remove authorizations for taxpayers who are no longer your clients. (See “Withdrawal of Representation” in Publication 947, Practice Before the IRS and Power of Attorney.)^{80, 81}

Recognize Phishing Scams

The best way to combat social engineering and phishing is heighten employee awareness—employees in your office must be educated on the dangers of phishing scams. These scams can result in cybercriminals taking over your computer or accounts to steal client data.

According to the IRS, a thief may pose as your tax software provider, your data storage provider, the IRS, or even as a prospective client. The thief may pose as your bank or as a professional colleague whose email was compromised. Thieves may hijack your email account to send spam emails under your name, tricking colleagues and clients into disclosing information. Generally, phishing or spear phishing emails have an urgent subject line. Example: Update Your Account Now. The objective is to entice you to open a link or an attachment:⁸²

- **Link:** The link may take you to a fake web page designed to look like a familiar website. Example: IRS e-Services. Again, there will be a call to action, such as “Click here NOW.” You may be asked to enter your username and password for an account, but you actually are disclosing your credentials to thieves—successful phishing campaigns almost always incorporate a sense of urgency to create fear.

⁸⁰ Authorization/access review is a basic IT Security control, and confirming EFIN/PTIN totals/removing unused CAF numbers reinforces this concept. Try to get into a habit of doing this when you have some downtime, maybe every Friday afternoon at 6 PM or so.

⁸¹ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁸² IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

- **Attachment:** The attachment may contain malicious computer code known as malware that can infect your computer and network systems. A common type of malware is keystroke tracking, which allows the criminal to see the words you type on your device, eventually disclosing your username and password to various accounts. In turn, this gives the criminal access to your tax software provider, bank, or encrypted client files.

A legitimate business will never email to request personal or sensitive information be sent to them via email, unless through a secured mail service—many firms now direct their clients and customers to secured web portals/websites with prompts to login with multi-factor authentication, but if there is a link always confirm the web address (URL) before clicking—also, call to verify if the request to log in is genuine.

Guard Against Phishing Emails

For this subsection of Publication 4557, the IRS offers specific anti-phishing training goals. As always, the goals here are the minimum level of awareness required by the IRS. The IRS explains that educated employees are the key to avoiding phishing scams, but these simple steps also can help protect against stolen data:⁸³

- Use separate personal and business email accounts. Protect email accounts with strong passwords and two-factor authentication if available. IT experts advise using multi-factor authentication (multiple passwords/IDs, and an independent verifying source—email/text/callback/prompts) instead of two-factor (generally only a password and ID). 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. Good practice is to make contact first by phone.
- Send only password-protected and encrypted documents if you must share files with clients via email. You can also use an encrypted share drive or an encrypted portal with required multi-factor authentication.
- Do not respond to suspicious or unknown emails. If it is IRS-related, forward to phishing@irs.gov.

Be Safe on the Internet

Browsing on the web has its own set of hazards, and the IRS has identified several items to implement or avoid in this section. The IRS recommends that you keep your web browser software up to date so that it has the latest security features, and that you should also:⁸⁴

⁸³ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

⁸⁴ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide for Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

- Scan files using your security software before downloading to your computer—always update your antivirus definitions (configure your antivirus solution to auto-update every 24 hours); delete your 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. The “S” stands for secure (e.g., <https://www.irs.gov>).—You should take caution, as this not always an indicator of a safe site). Additionally, it is good practice to avoid accessing business emails or information from public Wi-Fi connections. Use a VPN for additional security if you must public Wi-Fi.
- Disable stored password feature offered by some operating systems and web browsers such as Google and Firefox.
- Enable your browser’s pop-up blocker and do not call any number from pop-ups claiming your computer has a virus or click on tools claiming to delete viruses. Most of these pop-ups include a sense of urgency, and they often claim to be from Microsoft or the FBI.
- Do not download files, software, or applications from unknown websites. You may be inadvertently downloading a virus, malware, or spyware.
- If your browser’s homepage changes by itself, this could be a sign of malware or an intrusion. Review your last downloads and browser settings, check to see if you have anything new in your toolbar.

Report Data Loss to IRS/States (Breach Response/Notification)

According to the IRS, tax practitioners should report data losses or thefts immediately to the IRS—within the 24-hour reporting/notification requirement—so that appropriate precautions can be made to protect clients from fraudulent returns being filed in their names. You may want to contact your attorney and your cyber liability insurance representative as your first and second calls [practitioners should already have the order of calls/contacts established in their incident response plan (IRP)]. The steps below detail how to report data thefts to the IRS and law enforcement.⁸⁵

1. Contact the IRS and report client data theft to your local stakeholder liaison.
2. Contact the Federal Bureau of Investigation, your local office (if directed by the IRS).
3. Contact Secret Service, your local office (if directed by IRS).
4. Contact local police to file a police report on the data breach.
5. Contact 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.

⁸⁵ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide For Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

6. Contact State Attorneys General for each state in which you prepare returns. Most states require that the attorney general be notified of data breaches. Also, confirm with counsel all other applicable state breach notification and privacy requirements, including definitions, notice requirements, and defenses as part of your IRP or security plan;
7. Contact experts: Security expert—to determine the cause and scope of the breach, to stop the breach, and to prevent further breaches from occurring.⁸⁶ You should have your contact list ready as part of your IRP. Make sure you have an attorney or breach coach (a breach coach is usually an attorney with cybersecurity/IT experience) on your call list as well in order to determine appropriate breach response notification requirements.
8. Contact your insurance company/agent/broker—to report the breach and to check if your insurance policy covers data breach mitigation expenses.
9. Contact clients and other services (confirm with your attorney first if the breach or security incident requires notification to clients).
10. Contact the Federal Trade Commission. While the IRS specifies the FTC contact at idt-brt@ftc.gov, confirm the specific legal requirements for FTC breach notification with your attorney.
11. Contact your credit/ID theft protection agency. Certain states require offering credit monitoring/ID theft protection to victims of ID theft. Confirm with your attorney first.
12. Contact credit bureaus—to notify them if there is a compromise and clients may seek their services. Confirm with your attorney first.
 - a. Equifax Credit Information Services—Consumer Fraud Division

P.O. Box 105496
Atlanta, Georgia 30348-5496
Tel: (800) 997-2493
www.equifax.com
 - b. Experian

P.O. Box 2104
Allen, Texas 75013-2104
Tel: (888) EXPERIAN (397-3742)
www.experian.com

⁸⁶ For IRS notice, report any data theft or data loss to the appropriate IRS Stakeholder Liaison, <https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts>

c. Trans Union Fraud Victim Assistance Dept.

P.O. Box 390
Springfield, PA 19064-0390
Tel: (800) 680-7289
www.transunion.com;

13. Contact your clients—Before notifying clients of a security incident or a breach, confirm with legal counsel and, when possible, your forensic team, that this action is necessary. If so, send an individual letter to all victims to inform them of the breach but work with counsel, your insurance representative, and law enforcement on timing. (Clients should complete IRS Form 14039, Identity Theft Affidavit, only if they receive a notice/letter from the IRS or their e-filed return is rejected because of a duplicate Social Security number).

For a complete checklist, see Data Theft Information for Tax Professionals.⁸⁷

Again, do not forget that there will be at least one state breach notification requirement, as well as at least one state tax entity notification, with the possibility of FTC reporting as well. Contact your attorney to confirm all reporting requirements and also keep in mind the IRS 24-hour notification deadline.

Respond & Recover from a Data Loss

This section of Publication 4557 offer tips on business continuity after a breach or security incident, which include the following.⁸⁸

- Update your IRS Stakeholder Liaison with developments. IRS telephone assistants cannot accept third-party reports of identity theft. You should know the current identity and contact information for your stakeholder liaison and include this information in your IRP.
- Determine how the intrusion or theft occurred and make any required fixes before resuming tax preparation activities and being issued a new EFIN. You may need the services of a forensic expert, and the fees for these services are often in the tens or hundreds of thousands of dollars. Cyber liability insurance may pay the costs of breach investigation. Best practices suggest including the name of a forensic expert in your IRP and carrying cyber liability insurance.
- Develop a continuity plan (business continuity plan). Your plan should be up and running before a breach situation, not afterward.
- Make full backups of all business data and files. If you weren't doing it before the data loss, start as soon as your systems are clean. Performing routine backups will reduce the impact of a data loss or ransomware attack (as well as a hurricane or flood).

⁸⁷ <https://www.irs.gov/individuals/data-theft-information-for-tax-professionals>

⁸⁸ IRS Publication 4557, Safeguarding Taxpayer Data: A Guide for Your Business, <https://www.irs.gov/pub/irs-pdf/p4557.pdf>, Safeguarding Taxpayer Data: A Guide for Your Business.

- Encrypt backed-up files but don't lose the encryption key or forget your password. Consider a monthly, or more frequent, backup schedule during the filing season—ideally, real time or daily and incremental (incremental backups copy just the files/data modified or created since the last backup). You should also backup files after completing a routine system scan.
- Use an external hard drive or cloud storage. Encrypt files prior to uploading to the cloud.
- Consult with your professional insurance provider and your cyber liability insurance provider about data theft protection. Consult with this contact as soon as possible after purchasing your policy.
- Comply with the FTC Safeguards Rule (details can be found in the GLBA/FTC Rules in detail section). Review FTC's Data Breach Response: A Guide for Business for helpful guidance in notifying clients and tips for responding and recovering.⁸⁹
- Use the chart found at the end of Publication 4557 as a starting point if you do not already have a security plan in place.

IRS PUBLICATION 1345 (REV. 10-2021), HANDBOOK FOR AUTHORIZED IRS E-FILE PROVIDERS OF INDIVIDUAL INCOME TAX RETURNS

The second IRS publication to be examined in this chapter is Publication 1345, the Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,⁹⁰ which provides rules and requirements for participation in the IRS e-file program for individual income tax returns and related forms and schedules. The universe of all e-filer requirements is beyond the scope of this course, but we'll cover the most relevant cybersecurity sections. The IRS warns that violating a provision of this publication may subject the authorized IRS e-file provider (provider) to sanctions. The IRS further advises that providers should familiarize themselves with the Revenue Procedure 2007-40, 2007-26 IRB 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—note that these individual topics are beyond the scope of this course. The IRS revises Publication 1345 annually.⁹¹

The well-known Six Security and Privacy Standards are included in this publication, and online providers are required to comply with these standards.

Safeguarding the IRS e-file

Publication 1345 notes that safeguarding of an IRS e-file and related data from fraud and abuse is the shared responsibility of the IRS and Authorized IRS e-file Providers.

⁸⁹ <https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business>

⁹⁰ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹¹ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

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.⁹²

Publication 1345 defines **taxpayer data** 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).⁹³ If you become aware of unauthorized access or an attempt at unauthorized access of taxpayer data, you may need to report this event to the IRS and other state and federal regulatory bodies (i.e., state attorney general/tax department, the FTC, etc.) within each regulator's breach notification notice requirement (for the IRS, this is generally 24 hours).

As we will see in an upcoming chapter, the Federal Trade Commission (FTC) also works to protect taxpayer data. Providers subject to the Gramm-Leach-Bliley Act (GLBA) must follow the FTC's Financial Privacy and Safeguards Rule. The Safeguards Rule requires the protection of the security, confidentiality and integrity of customer (taxpayer) 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. FTC and GLBA requirements in detail follow in a later section of this course.⁹⁴

Publication 1345 mentions that Pub. 4557 (our previous publication) includes information about security standards and best practice guidelines to safeguard consumer information such as personal tax data, and adds that failing to take necessary steps to implement or correct your security program may result in sanctions from the FTC. Failures that lead to an unauthorized disclosure may subject you to penalties under sections 7216 and/or 6713 of the IRC. We have already covered Publication 4457, and the additional FTC guidance is covered separately below. The IRS uses the GLBA privacy and security standards, and GLBA is enforced by the FTC, which has levied fines and penalties to non-compliant entities.⁹⁵

More importantly, providers must appoint an individual as a responsible official, often a Chief Information Security Officer (CISO), who is responsible for ensuring the provider firm meets IRS e-file rules and requirements. Providers with problems involving fraud and abuse may be suspended or expelled from participation in IRS e-file, be assessed civil and preparer penalties or be subject to legal action. Again the FTC and state regulators may also pile on additional fines, penalties, and enforcement actions.⁹⁶

⁹² <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹³ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹⁴ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹⁵ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹⁶ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

IRS e-file Security, Privacy & Business Standards

The IRS has mandated six security, privacy, and business standards to supplement the Gramm-Leach-Bliley Act to protect their information collected, processed, and stored by online providers of individual income tax returns. Individual income tax returns generally refer to the 1040 family of returns (you may refer to the IRS Publication 3112, IRS e-file Application and Participation, for definition of online provider, but the detailed criteria relating to an online provider is beyond the scope of this course). 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.⁹⁷

According to the IRS, these standards also address certain business and customer service objectives such as instant payment options access to website owner/operator's contact information, and online provider's written commitment to maintaining physical, electronic, and procedural safeguards of taxpayer information that comply with applicable law and federal standards.⁹⁸

The Security Standards⁹⁹

1. Extended Validation SSL Certificate.¹⁰⁰ Your website must be secure—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.
2. External Vulnerability Scan. The IRS requires that online providers of individual income tax returns must 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 (PCI-DSS or PCI for short). All scans must 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).¹⁰¹ In addition, online providers of individual income tax returns whose systems are hosted shall

⁹⁷ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹⁸ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

⁹⁹ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹⁰⁰ TLS 1.0 or later (most recent version is up to 1.3 as of 2019) is the preferred security standard currently in use.

¹⁰¹ https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

ensure that their host complies with all applicable requirements of the PCI-DSS—make sure your host vendor contract includes this requirement. For the purposes of this standard, system components is defined as any network component, server, or application that is included in or connected to the taxpayer data environment. The taxpayer data environment is that part of the network that possesses taxpayer data or sensitive authentication data. If scan reports reveal vulnerabilities, action shall (the ultimate meaning here is must) be taken to address the vulnerabilities in line with the scan report's recommendations. Retain weekly scan reports for at least one year. The ASV and the host (if present) **must** be in the United States.

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—as opposed to #2 previously, which addresses external hosts. 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.
4. 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.¹⁰²
5. Website Challenge-Response Test. The next 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;¹⁰³

Be aware that CAPTCHA had a security flaw, which was patched.¹⁰⁴ Also, Google has created a new tool (reCAPTCHA 3.0: "...easy on people, hard on bots").¹⁰⁵

6. 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—again, not externally hosted. 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;¹⁰⁶

¹⁰² See <http://www.privacyalliance.org/resources/> and <https://www.irs.gov/e-file-providers/privacy-seal-providers-acceptable-to-irs>

¹⁰³ <https://support.google.com/a/answer/1217728?hl=en>

¹⁰⁴ <https://www.zdnet.com/article/google-patches-recaptcha-bypass-vulnerability/>

¹⁰⁵ <https://www.google.com/recaptcha/intro/v3.html>

¹⁰⁶ See <https://makeawebsitehub.com/reviews/domain-registrars/> for basic domain name registrar information

7. **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. See instructions in other chapters for submitting incident reports. 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.¹⁰⁷

Safeguarding IRS e-file from Fraud & Abuse¹⁰⁸

The IRS has stated that safeguarding taxpayer and IRS e-file from identity-theft refund fraud requires that providers be diligent in detecting and preventing identity-theft fraud patterns and schemes. In fact, Electronic Return Originators (EROs) must be particularly diligent while acting in their capacity as the primary 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. EROs can find additional information in the article "Reporting Fraud and Abuse Within the IRS e-file Program."

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. A fraudulent return is a return in which the individual is attempting to file using someone else's name or SSN on the return or the taxpayer is presenting documents or information that have no basis in fact. A potentially abusive return is a return that the taxpayer is required to file but contains inaccurate information that may lead to an understatement of a liability or the overstatement of a credit resulting in a refund to which the taxpayer may not be entitled.

CPA practitioners are also under separate AICPA confidentiality requirements, and should confirm these requirements when a reporting situation occurs relating to a client.¹⁰⁹

Verifying Taxpayer Identity & Taxpayer Identification Numbers (TINs)¹¹⁰

The IRS states that 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. An ERO should ask taxpayers not known to them to provide two forms of identification

¹⁰⁷ <https://www.irs.gov/e-file-providers/instructions-for-reporting-web-site-security-incidents-updated-10-02-08>

¹⁰⁸ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 11-2020).

¹⁰⁹ AICPA Code of Professional Conduct, Section 1.700.001—CPA practitioners must also consider these items as well with taxpayer confidentiality situations, including during reportable breach/security incident occurrences.

¹¹⁰ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

(picture IDs are preferable) that include the taxpayer's name and current or recent address.¹¹¹

The IRS requires that the TIN entered in the Form W-2, Wage and Tax Statement, in the electronic return record must be identical to the TIN on the version provided by the taxpayer. Accordingly, the TIN on the Form W-2 should be identical to the TIN on the electronic return unless otherwise allowed by the IRS. The IRS requires taxpayers filing tax returns using an ITIN to include the TIN, usually a SSN, shown on Form W-2 from the employer in the electronic record of the Form W-2. This may create an identification number (ITIN/SSN) mismatch as taxpayers must use their correct ITIN as their identifying number in the individual income tax return. The IRS e-file system can accept returns with this identification number mismatch. EROs should enter the TIN/SSN in the electronic record of the Form W-2 provided to them by taxpayers. Software must require the manual key entry of the TIN as it appears on Form W-2 reporting wages for taxpayers with ITINs. EROs should ascertain that the software they use does not auto-populate the ITIN in the Form-W-2 and if necessary, replace the ITIN with the SSN on the Form W-2 the taxpayer provided.¹¹²

According to the IRS, incorrect TINs, using the same TIN on more than one return or associating the wrong name with a TIN are some of the most common causes of rejected returns (see "Acknowledgements of Transmitted Return Data" in "ERO Duties After Submitting the Return to the IRS").¹¹³

Providers should name control and TINs identify taxpayers, spouses and dependents. A **name control** is the first four significant letters of an individual taxpayer's last name or a business name as recorded by the Social Security Administration (SSA) or the IRS. Having the wrong name control in the electronic return record for a taxpayer's TIN contributes to a large portion of TIN related rejects. The most common example for a return rejecting due to a mismatch between a taxpayer's TIN and name control involves newly married taxpayers. Typically, the taxpayer may file using a correct SSN along with the name used in the marriage, but the taxpayer has failed to update the records with the SSA to reflect a name change. To minimize TIN related rejects, it is important to verify taxpayer TINs and name control information prior to submitting electronic return data to the IRS.¹¹⁴

Be Aware of Non-Standard Information Documents¹¹⁵

Providers should be cognizant of the fact that the IRS has identified questionable Forms W-2 as a key indicator of potentially abusive and fraudulent returns (see Safeguarding IRS e-file from Fraud and Abuse above). Be aware of suspicious or altered Forms W-2,

¹¹¹ If you are retaining a copy of this personal data, ensure that you are either keeping the paper copy in a locked drawer with limited key access or keeping a digital copy on an encrypted drive, password protected drive, or keeping the individual digital copy itself encrypted. All drive access should require multi-factor authentication.

¹¹² <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹¹³ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹¹⁴ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹¹⁵ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

W-2G, 1099-R, and forged or fabricated documents. 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.¹¹⁶

Providers should report questionable Forms W-2 if they observe or become aware of them. See "Reporting Fraud and Abuse Within the IRS e-file Program." But for CPA tax practitioners, there may be a consent for disclosure/reporting issue here, which is beyond the scope of this course.¹¹⁷

Refund Returns¹¹⁸

According to Publication 1345, 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.

Direct Deposit of Refunds¹¹⁹

Additionally, 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.

Electronic Signature Guidance for Forms 8878 & 8879¹²⁰

According to the IRS, 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 ERO must meet certain requirements

¹¹⁶ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹¹⁷ See <https://www.thetaxadviser.com/issues/2018/feb/ethics-rule-suspected-illegal-acts-clients.html>

¹¹⁸ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹¹⁹ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹²⁰ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

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. Publication 1345 gives examples of currently acceptable electronic signature methods.

Electronic Signature Guidance for Forms 8878 & 8879¹²¹

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.¹²²

Identity assurance levels

According to NIST, 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 (LOA). NIST defines three LOAs for the identity proofing process—1, 2, and 3—in increasing order of their strengths—the IRS requires Level 2 or stronger).¹²³

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

¹²¹ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹²² Also see update at 800-63-A, on Enrollment and Identity Proofing, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>

¹²³ NIST Publication 800-63-A, on Enrollment and Identity Proofing, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>

service provider may collect biometrics for the purposes of non-repudiation and re-proofing.

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 can 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 addition, 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 IAL3.¹²⁴ Biometric data is within the definition of personal data or PII, and must be securely stored, used, and transferred under several state laws.

Identity verification requirements & 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).

¹²⁴ Security Boulevard, Archit Lohokare, July 9, 2019, NIST 800-63-A: Enrollment and Identity Proofing,

Source: Security Boulevard, Archit Lohokare, July 9, 2019, NIST 800-63-A: Enrollment and Identity Proofing, <https://securityboulevard.com/2019/07/nist-800-63-a-enrollment-and-identity-proofing/>

Electronic Records¹²⁵

Modification of original electronic records is a major concern for all businesses. The IRS requires that electronic signatures must be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record. After an electronic record has been signed, it must be made tamper-proof. The document must be locked down to prevent it from being modified. Storage systems must have secure access controls to ensure that the electronic records cannot be modified.

Additionally, storage systems must also contain a retrieval system that includes an indexing system, and the ability to reproduce legible and readable hardcopies of electronically stored records.

Internet Protocol Information¹²⁶

The IRS requires that Internet Protocol (IP) information of the computer the ERO uses to prepare the return (or originate the electronic submission of collected returns) must be included in all individual income tax returns. The required Internet Protocol information includes: public/routable IP address, IP date, IP time, and IP time zone.

The IRS continues: with many different ERO e-filing business models, the computer used to prepare (or originate the electronic submission of collected returns) may not have a public/routable IP address. If the computer used for preparation (or origination of the electronic submission of collected returns) is on an internal reserved IP network, then the IP address should be the public/routable IP address of the computer used to submit the return. If the computer used for preparation (or origination of the electronic submission of collected returns) is used to transmit the return to the IRS, then the IP address should be the public/routable IP address of that computer. If it is not possible to capture the public/routable IP address, then the ERO or software may have to hard code the IP address into each return. The IRS will reject individual income tax returns e-filed without the required IP address. Any return received by the IRS containing a private/non-routable IP address will be flagged in the Acknowledgement File with an R in the Reserved IP Address Code field of the ACK key record indicating that a reserved IP address is present for the return.

The IRS has implemented a Device ID field for electronic return filers and preparers. The IRS will utilize this unique identifier; in addition to key elements already collected to improve fraud and ID theft detection. Vendors implementing Device ID in their software should ensure that their privacy notice will cover Device ID.

¹²⁵ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹²⁶ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

ERO Duties After Submitting the Return to the IRS¹²⁷

Record keeping & documentation requirements

EROs must retain the following material until the end of the calendar year at the business address from which it originated the return or at a location that allows the ERO to readily access the material as it must be available at the time of IRS request. An ERO may retain the required records at the business address of the responsible official or at a location that allows the responsible official to readily access the material during any period of time the office is closed, as it must be available at the time of IRS request through the end of the calendar year.

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.

The submission ID can be added to the Form 8879 and 8878 or the acknowledgment containing the submission ID can be associated with Forms 8879 and 8878.

If the acknowledgement is used to identify the submission ID, the acknowledgement must be kept in accordance with published retention requirements for Forms 8879 and 8878. The acknowledgement is not required to be physically attached to Form 8879 and 8878; it can be electronically stored.

The IRS allows EROs to electronically image and store all paper records they are required to retain for IRS e-file. This includes Forms 8453 and paper copies of Forms W-2, W-2G, and 1099-R as well as any supporting documents not included in the electronic record and Forms 8879 and 8878. The storage system must satisfy the requirements of Revenue Procedure 97-22, 1997-1 C.C. 652, Retention of Books and Records. In brief, the electronic storage system must ensure an accurate and complete transfer of the hard copy to the electronic storage media. The ERO must be able to reproduce all records with a high degree of legibility and readability (including the taxpayers' signatures) when displayed on a video terminal and when reproduced in hard copy.

Disposal of Taxpayer Information¹²⁸

Publication 1345 requires that providers must comply with records retention policies standards for retaining the required records (electronic and paper format) for the required period, and that taxpayer information and sensitive data files must be destroyed

¹²⁷ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 11-2020).

¹²⁸ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

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 5mm (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—confirm with your attorney and ensure you are familiar with these laws as well.

Transmission¹²⁹

Reporting of potential identity theft refund fraud activity

The IRS requires that providers be diligent in detecting and preventing identity-theft fraud patterns and schemes. Early detection of these patterns and schemes is critical to stopping them and their adverse impacts, and to protecting taxpayers and IRS e-file. Providers who transmit more than 2,000 individual income tax returns per year are required to perform analysis to identify 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.

NOTE: For CPA tax practitioners, there may be a consent for disclosure/reporting issue here.¹³⁰

Additional transmission requirements¹³¹

The IRS states that in fulfilling the requirements of an authorized IRS e-file provider (Provider) participating in IRS e-file, transmitters must perform the following actions:

1. Transmit all electronic portions of returns to the appropriate IRS center within three calendar days of receipt. Note: 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
2. Retrieve the acknowledgment file within two work days of transmission.
3. 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 ERO or Intermediate Service Provider within two work days of retrieving the acknowledgment file.

¹²⁹ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹³⁰ <https://www.thetaxadviser.com/issues/2018/feb/ethics-rule-suspected-illegal-acts-clients.html>.

¹³¹ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

4. Retain an acknowledgment file received from the IRS until the end of the calendar year in which the electronic return was filed.
5. 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.
6. Promptly correct any transmission error that causes an electronic transmission to be rejected.
7. 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.
8. Ensure the security of all transmitted data.
9. 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.
10. Use only software that does not have an IRS assigned production password built into the software.
11. Provide the Device ID from the equipment used to prepare the return.
12. Providers who collectively transmit more than 2,000 individual income tax returns per year are required to perform analysis to identify potential identity-theft fraud patterns and schemes. They must 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. NOTE: For CPA tax practitioners, there may be a consent for disclosure/reporting issue here, which is beyond the scope of this course.¹³²

Disclosure of Tax Return Information¹³³

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 IRC §7216 and/or the civil penalties in IRC §6713 for unauthorized disclosure or use of tax return information. Also, CPA practitioners must comply with additional AICPA rules protecting client confidentiality.¹³⁴

¹³² <https://www.thetaxadviser.com/issues/2018/feb/ethics-rule-suspected-illegal-acts-clients.html>

¹³³ <https://www.irs.gov/pub/irs-pdf/p1345.pdf>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 10-2021).

¹³⁴ AICPA Code of Professional Conduct, Section 1.700.001, CPA practitioners must also consider these items as well with taxpayer confidentiality situations, including during reportable breach/security incident occurrences.

IRS PUBLICATION 5293, PROTECT YOUR CLIENTS; PROTECT YOURSELF; DATA SECURITY RESOURCE GUIDE FOR TAX PROFESSIONALS¹³⁵

Our third IRS cybersecurity-related document for this chapter is Publication 5293, Protect Your Clients; Protect Yourself; Data Security Resource Guide for Tax Professional. This brief document includes security requirements applicable to taxpayer data and several definitions relating to data security.

Publication 5293 refers to Publications 4557, 1345, and the NIST document which appears in the next chapter.

Publication 5293 reminds tax practitioners that The Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act (GLBA), requires practitioners to create and maintain a security plan for the protection of client data—GLBA details will be covered in a separate section below.

The next section of the publication discusses how to review internal controls in the context of cybersecurity controls over taxpayer data, including the following:¹³⁶

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never click on/open a link or any attachment from a suspicious email. The IRS never initiates initial email contact with tax practitioners about returns, refunds or requests for sensitive financial or password information –employee training would be appropriate for these activities;
- Create a data security plan using IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security—The Fundamentals, by the National Institute of Standards and Technology;
- Review internal controls: Install anti-malware/antivirus security software on all devices (laptops, desktops, routers, tablets and phones) and keep software set to automatically update—these areas are covered in the respective documents;
- Use strong and unique passwords of 8 (12-14 suggested as best practices) or more mixed characters, password protect all wireless devices, use a phrase or words that are easily remembered and change passwords periodically—also use a password manager or vault;

¹³⁵ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E.

¹³⁶ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E).

- Encrypt all sensitive files/emails and use strong password protections—use TLS for email and encrypt the hard drives of all desktops and mobile devices which contain taxpayer or other sensitive data;
- Back up sensitive data to a safe and secure external source not connected fulltime to a network—back up both full and incrementally on a regular basis, and back up to an external device which is securely stored and encrypted and/or to the cloud;
- 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 -also follow applicable state data disposal laws;
- Limit access to taxpayer data to individuals who need to know—implement a role-based identity access policy/procedure/controls;
- 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—but you should confirm any overriding confidentiality rules or laws that may apply, especially for CPA practitioners;
- Stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts and Social Media.

Publication 5293 continues with the “Learn the Signs of Data Theft” section, which focuses on common clues to and indications of data theft:¹³⁷

- Client e-filed returns begin to reject because returns with their Social Security numbers were already filed;
- Clients who haven’t filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS;
- Clients who haven’t filed tax returns receive refunds; Clients receive tax transcripts that they did not request;
- Clients who created an IRS online 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;
- The number of returns filed with tax practitioner’s Electronic Filing Identification Number (EFIN) exceeds number of clients—again, it is a requirement to check this weekly;

¹³⁷ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E.

- Tax professionals or clients responding to emails that practitioner did not send;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without someone touching the keyboard;
- Network computers locking out tax practitioners.

Next up is the Stay Vigilant section, which spells out proactive steps to take to uncover fraud or data theft. Again, these are required actions:¹³⁸

- Track your daily e-File acknowledgements. If there are more acknowledgements than returns you know you filed, dig deeper;
- Track your weekly EFIN usage. The number of returns filed with your Electronic Filing Identification Number (EFIN) is posted weekly. Go to your e-Services account, access your e-file application and check “EFIN Status.” If the numbers are off, contact the e-Help desk. Keep your EFIN application up-to-date with all phone, address or personnel changes;
- If you are a ‘Circular 230 practitioner’ or an ‘annual filing season program participant’ and you file 50 or more returns a year, you can check your PTIN account for a weekly report of returns filed with your Preparer Tax Identification Number (PTIN.) Access your PTIN account and select “View Returns Filed Per PTIN.” File Form 14157, Complaint: Tax Return Preparer, to report excessive using your PTIN 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. See Publication 947, Practice Before the IRS and Power of Attorney;
- Create your IRS online accounts using the two-factor Secure Access authentication, which helps prevent account takeovers. See IRS.gov/secure access to review necessary steps—IT experts advise using Multi-Factor Authentication, (multiple passwords/ IDs, and an independent verifying source—email/text/callback/prompts), instead of Two Factor (generally a Password and ID).

¹³⁸ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E.

Publication 5293 continues with “Report Lost or Stolen Data Quickly”—make sure that you have processes in place to notify the IRS of a reportable security incident or breach of taxpayer data within 24 hours as well as to complete these additional actions:¹³⁹

- Contact the IRS and law enforcement (best practices suggest that practitioners contact their attorney or insurance carrier as the first contact made after a breach –this step should be documented in their Incident Response Plan):
- Internal Revenue Service, report client data theft to your local Stakeholder Liaison;
- Federal Bureau of Investigation, your local office (if directed.);
- Secret Service, your local office (if directed.);
- Local police—To file a police report on the data breach;
- Contact 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;
- State Attorneys General for each state in which you prepare returns. Most states require that the attorney general be notified of data breaches—State laws may require additional notifications—confirm, with your attorney, the state law breach notification requirements in the state/s applicable to your practice;
- Contact experts: Security expert—to determine the cause and scope of the breach, to stop the breach and to prevent further breaches from occurring;
- Insurance company—to report the breach and to check if your insurance policy covers data breach mitigation expenses, if you carry cyber liability insurance—there may be a notification requirement to trigger coverage, so the insurance representative should be the first or second contact/call you should make after discovering a reportable incident. Your attorney should also be one of the first to be notified.

¹³⁹ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E.

Stay Connected¹⁴⁰

The final section of Publication 5293 is entitled “Stay Connected,” which includes links to several key IRS cybersecurity websites with up-to-date information. 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.¹⁴¹

- **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;

IRS Security Bookmarks:

- Identity Protection: Prevention, Detection and Victim Assistance—Main identity theft page;
- Data Theft Information for Tax Professionals—How to report client data loss to the IRS;
- Protect Your Clients; Protect Yourself—Awareness campaign and scam alerts for tax pros;
- Taxes. Security. Together.—Awareness campaign for taxpayers;
- Identity Theft Information for Tax Professionals—An overview;
- Report Phishing and Online Scams—How to report IRS-related scams;
- How IRS Identity Theft Victim Assistance Works—What clients can expect;
- Maintain, Monitor and Protect Your EFIN—Protect your IRS-issued identification numbers;
- Secure Access—How to authenticate your identity to access IRS online tools;

¹⁴⁰ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E.

¹⁴¹ <https://www.irs.gov/pub/irs-pdf/p5293.pdf>, Protect Your Clients; Protect Yourself, Data Security Resource Guide for Tax Professionals, Catalog Number 71256E.

- Security Summit—Track safeguards enacted by IRS, states and industry;
- Newsroom—Stay in the know by subscribing to IRS News Releases;
- Stakeholder Liaisons Local Contact—find your local contact to report data losses.

TAX SECURITY 2.0—A "TAXES-SECURITY-TOGETHER" CHECKLIST—STEPS 1-5 (IR-2019-127, JULY 16, 2019)¹⁴²

Step 1

The initial step on the checklist involves mandatory protections, with detailed commentary in several areas. These topics fall into several major security categories:¹⁴³

1. **Antivirus software.**¹⁴⁴ Although details may vary between commercial products, antivirus software scans computer files or memory for certain patterns that may indicate the presence of malicious software (also called malware). Antivirus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware from cyber criminals. Antivirus vendors find new issues and update malware daily, so it is important that people have the latest updates installed on their computer, according to the U.S. Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security. Once users have installed an antivirus package, they should scan their entire computer periodically by performing:
 - Automatic scans—Most antivirus software can be configured to automatically scan specific files or directories in real time and prompt users at set intervals to perform complete scans.
 - Manual scans—If the antivirus software does not automatically scan new files, users should manually scan files and media received from an outside source before opening them. This manual process includes:
 - Saving and scanning email attachments or web downloads rather than opening them directly from the source;
 - Scanning portable media, including CDs and DVDs, for malware before opening files;
 - Keeping security software set to automatically receive the latest updates/patches so that it is always current.¹⁴⁵

¹⁴² <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁴³ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁴⁴ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁴⁵ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

2. **Firewalls.**¹⁴⁶ Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary web traffic and preventing malicious software from accessing your systems. Firewalls can be configured to block data from certain suspicious locations or applications while allowing relevant and necessary data through, according to US-CERT. Firewalls may be broadly categorized as hardware or software. While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use:

- Hardware—Typically called network firewalls, these external devices are positioned between a computer and the internet (or another network connection). Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them;
- Software—Most operating systems include a built-in firewall feature that should be enabled for added protection even if using an external firewall. Firewall software can also be obtained as separate software from a local computer store, software vendor or ISP. If downloading firewall software from the internet, make sure it is from a reputable source (such as an established software vendor or service provider) and offered via a secure website.

3. **Two-factor authentication—multi-factor authentication is preferred as a best practice and is now a requirement for all tax software providers.**¹⁴⁷

Many email vendors now offer their customers two-factor authentication protections to access email accounts. Tax practitioners should **always** use this option to prevent their accounts from being taken over by cybercriminals and otherwise putting their clients and colleagues at risk.

Two-factor authentication helps by adding an extra layer of protection beyond a password. Often two-factor authentication means the returning user must enter credentials (username and password) plus another step, such as entering a security code sent via text to a mobile phone. An attacker may be able to steal the username and password but it would be highly unlikely that the attacker would also have a user's mobile phone to receive a security code and complete the process.

The use of two-factor authentication or three-factor authentication is on the rise, and **tax practitioners should always select multi-factor authentication protection when it is offered**, whether on an email account or with tax software or with any password-protected product—Practitioners can check their email account settings to see if the email provider offers two-factor protections.

IRS Secure Access, which protects IRS.gov tools including e-Services, is an example of two-factor authentication.

4. **Backup software/services.**¹⁴⁸ Critical files on computers should routinely be backed up to external sources. A copy of the file is made and stored either online as part of a cloud storage service or similar product. Another external source is

¹⁴⁶ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁴⁷ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁴⁸ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

comprised of external disk drives, which include multiple terabytes of storage capacity. Tax professionals should ensure that taxpayer data that is backed up also is encrypted.

Also, for best IT practices, establish a chain of custody/data inventory of critical files—critical files/critical data should be identified beforehand. If a file includes personal data/PII such as social security number/name/address/email address, tax data, etc., it should be placed in a high-risk classification (confidential/private/sensitive, etc.). Data Classification tools may help practitioners in this area.

5. **Drive encryption.**¹⁴⁹ Given the sensitive client data maintained on tax practitioners' devices (including desktops and laptops/other mobile devices), users should encrypt all devices with full disk encryption. Full disk encryption is applied to the data, applications and the operating system on a device. Users are prompted to enter a disk encryption key, which is similar to a password, when a device boots up in order to access data and applications on the device.
6. **Virtual Private Network.**¹⁵⁰ If a practitioner's employees must occasionally connect to unknown networks or work from home, set up an encrypted Virtual Private Networks (VPN) to allow for a more secure connection into the practitioner's network. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the practitioner's network. Search for "Best VPNs" to find a legitimate vendor; major technology sites often provide lists of "top" or "best" services. Practitioners should install, on a regular frequency, the most recent patches and updates for their VPN.

Step 2

Step 2 centers on GLBA/FTC safeguards over taxpayer data and confidentiality requirements for tax practitioners (as discussed elsewhere in this course, CPA practitioners are required to comply with AICPA client confidentiality rules).¹⁵¹

Step 2 starts off with the requirement to create a data security plan under federal law, and notes that many in the tax professional community do not realize they are required under federal law to have a data security plan:¹⁵²

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley (GLB) Act, 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

¹⁴⁹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁵⁰ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>

¹⁵¹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-2>

¹⁵² <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-2>

rules for tax practitioners participating as an Authorized IRS e-file Provider.

The FTC-required information security 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. According to the FTC, each company, as part of its plan, must do the following:

- 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 practitioner's operation and evaluate the effectiveness of the current safeguards for controlling these risks (conduct a risk assessment);
- Design and implement a safeguards program and regularly monitor and test it;
- Select service providers (vendors) which maintain appropriate safeguards, and make sure the contract requires them to maintain safeguards and to oversee their handling of customer information—basic IT vendor oversight; and
- Evaluate and adjust the security plan in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring—testing and monitoring should include an annual risk assessment, which tests the design and effectiveness of your cybersecurity controls.

GLBA/FTC's Safeguards Rule requires practitioners to assess and address the risks to customer information in all areas of their operations;

Please note: The FTC currently is re-evaluating the Safeguards Rule and has proposed new regulations. Be alert to any changes in the Safeguards Rule and its effect on the tax practitioner community. 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, states: Safeguarding of the 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 fraud and abuse, reporting it to the IRS, and preventing it when possible. Providers must also cooperate with the IRS' investigations by making available to the IRS upon request information and documents related to returns with potential fraud or abuse.^{153, 154}

¹⁵³ For CPA tax practitioners, there may be a consent for disclosure/reporting issue here, which is beyond the scope of this course.

¹⁵⁴ See <https://www.thetaxadviser.com/issues/2018/feb/ethics-rule-suspected-illegal-acts-clients.html>

- 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 GLBA and the FTC's implementing rules and regulations, 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.

Many state laws govern or relate to the privacy and security of financial data, which includes taxpayer data, and these laws have strict notice and reporting requirements. They extend rights and remedies to consumers by requiring individuals and businesses that offer financial services to safeguard nonpublic personal information. Tax practitioners must also be cognizant that all 50 states now have data breach notification laws that require notification to individuals and regulatory agencies if certain thresholds are met.¹⁵⁵ For more information on state laws that businesses must follow, consult your attorney/counsel. You must know which state tax and non-tax entities to contact in the case of a reportable security incident or breach—this information should be in your IRP (Incident Response Plan) before a reportable event occurs. To notify the IRS in case of data theft, contact the appropriate local IRS Stakeholder Liaison.

In some states, data breaches must be reported to various authorities. Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the state tax entities.¹⁵⁶

Step 3

Step 3 focuses on Social Engineering and Phishing. The continuing threat of phishing emails (social engineering remains the most common tactic used by cybercriminals to steal sensitive data).¹⁵⁷ You are only as safe as your least educated employee. More than 90% of all data thefts start with a phishing email.¹⁵⁸ Employees may open a link that goes to a fake site or may open an attachment that is embedded with malware that secretly downloads onto their computers.

Tax practitioners are often targeted victimized after being targeted in an attack known as spear phishing. The objective of a spear phishing email is to pose as a trusted source and

¹⁵⁵ <https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws>

¹⁵⁶ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-2>

¹⁵⁷ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-3>

¹⁵⁸ [https://assets.barracuda.com/assets/docs/dms/18981_Barracuda_EmailProtect_Infographic_\(3\).pdf](https://assets.barracuda.com/assets/docs/dms/18981_Barracuda_EmailProtect_Infographic_(3).pdf)

bait the recipient into opening an embedded link or an attachment. The email may make an urgent request to the tax practitioner to update an account immediately. A link may seem to go to another trusted website, for example a cloud storage or tax software provider login page, but it's actually a website controlled by the attacker.

An attachment may contain malicious software that logs monitors and captures keystrokes and the victim's passwords along with other login information. Additionally, attackers may be able to even take remote control of the victim's computers and or sever.

Common spear phishing scams observed by the IRS include thieves posing as prospective clients who send 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.¹⁵⁹

The IRS has also observed attackers posing as tax software providers or data storage providers who send emails containing links that go to web pages that mirror genuine websites. The thieves' goal is to trick tax practitioners into entering their usernames and passwords into these fake sites, which are then stolen.

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.¹⁶⁰

Educated employees are the key to avoiding phishing scams, and office systems are only as safe as the least informed employee. 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—Multi-Factor Authentication is preferred as an IT best practice.
- 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 telephone.
- Send only password-protected and encrypted documents if any files must be shared with clients via email (use TLS).

¹⁵⁹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-3>

¹⁶⁰ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-3>

- Do not respond to suspicious or unknown emails; if the email is IRS-related, forward to phishing@irs.gov.
- **Don't click the link!**

Step 4

Step 4 includes guidance relating to ransomware and client data theft.

Another trick used by thieves is rather than stealing the data, they encrypt it, in 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.¹⁶¹

Initial ransomware signs can be as subtle as an unusually slow computer system or as obvious as multiple clients all unexpectedly receiving an identical IRS notice.

Recognize the signs of client data theft¹⁶²

The IRS and Summit partners have created a list of warning signs that a tax practitioner or the practitioner's office may have experienced a data theft:

- Client e-filed returns start to be rejected by the IRS or state tax agencies because returns with their Social Security numbers were already filed.
- Clients who have not 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 disabled¹⁶³ or clients unexpectedly receive an IRS notice that an IRS online account was created in their names.
- The number of returns filed with the tax professional's Electronic Filing Identification Number (EFIN) exceeds the number of clients.
- Tax practitioners or clients responding to emails that the firm did not send.
- Network computers are running slower than normal.

¹⁶¹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>.

¹⁶² <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>.

¹⁶³ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

- Computer cursors are moving or changing numbers without someone touching the keyboard.
- Network computers are locking out employees.¹⁶⁴

Because IRS and state tax systems will only accept one unique Social Security number, taxpayers often discover they are a victim when they attempt to e-file and receive a notice that their tax return has been rejected because a return with their SSN already is in the system. Or, more commonly, the IRS identifies a return that could be an identity theft return and sends a letter to the taxpayer asking them to contact the agency to let the IRS know if they filed the return.¹⁶⁵

Identity thieves sometimes try to leverage the stolen data by using taxpayer information to access the IRS Get Transcript system. Taxpayers who receive transcripts by mail but did not order them are sometimes victims of this approach. Get Transcript Online is protected by a robust, two-factor authentication process. Criminals may still try to use stolen identities to try to create Get Transcript accounts, which results in the IRS disabling the account and sending the taxpayer a letter.¹⁶⁶

During the tax filing season, tax providers should perform a weekly review of returns filed with the office's EFIN. A report is updated weekly. Tax providers can access their e-file applications and select "check EFIN status" to see a count. If the numbers are inflated, providers should contact the IRS e-Help Desk. Tax professionals may also notice IRS acknowledgements for returns they did not e-file. Acknowledgements are sent soon after a return is transmitted.¹⁶⁷

Tax practitioners who fall victim to spear phishing email scams may suddenly see responses to emails they never sent. If a practitioner mistakenly provides a username and password to the thief, the thief often harvests the practitioner's contact list, stealing names and email addresses of colleagues and clients which enables the attackers to use the tax firm to expand their spear phishing scam.

Always be alert to phishing scams, even if the emails appear to come from a colleague or client. If the language sounds a bit off or if the request seems unusual, contact the "sender" by telephone to verify rather than opening a link or attachment;

There are several signs that office computer systems may be under attack or may be under remote control, such as the cursor moving with no one at the keyboard. The IRS is aware of many examples in which cybercriminals gain access to practitioners' office computers, complete the pending Form 1040s, change electronic deposit information to their own accounts, and then e-filed the returns—all performed remotely.

Tax professionals who notice any signs of identity theft should contact their state's IRS Stakeholder Liaison immediately—no later than 24 hours after becoming aware of the reportable breach or security incident. The process for reporting data theft to the IRS is

¹⁶⁴ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

¹⁶⁵ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

¹⁶⁶ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

¹⁶⁷ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

outlined in Data Theft Information for Tax Professionals and elsewhere in this course manual.

Security Incidents and breaches must also be reported to state tax and non-tax regulatory entities. To help tax practitioners find where to report data security incidents at the state level, email the Federation of Tax Administrators at statealert@taxadmin.org. Always call your attorney as part of your Incident Response Plan when you become aware of a security incident or breach.¹⁶⁸

Step 5

Step 5 discusses the topic of recognizing signs of client data theft with proactive actions practitioners can take. There are many similar or identical items in the other Step documents as well as in the publications we have already explored.

During the tax filing season, tax providers should perform a weekly review of returns filed with the office's EFIN. A report is updated weekly. Providers can access their e-file applications and select "check EFIN status" to see a count. If the numbers are inflated, providers should contact the IRS e-Help Desk. Tax professionals may also notice IRS acknowledgements for returns they did not e-file. Acknowledgements are sent soon after a return is transmitted.¹⁶⁹

Tax practitioners who fall victim to spear phishing email attacks may suddenly see responses to emails they never sent. If a practitioner mistakenly provides username and password information to the thief, the thief often harvests the practitioner's contact list, stealing names and email addresses of colleagues and clients and enabling the crooks to use the tax firm to expand their spear phishing scam.¹⁷⁰

Always be alert to phishing scams, even if the emails appear to come from a colleague or client. If the language sounds a bit off or if the request seems unusual, call the sender to verify rather than opening a link or attachment.¹⁷¹

There are several signs that office computer systems may be under attack or may be under remote control, such as the cursor moving with no one at the keyboard. The IRS is aware of many examples in which cybercriminals gain access to practitioners' office computers, complete the pending Form 1040s, change electronic deposit information to their own accounts, and then e-filed the returns—all performed remotely.¹⁷²

Tax practitioners who notice any signs of identity theft should contact their state's IRS Stakeholder Liaison immediately. The process for reporting data theft to the IRS is outlined in Data Theft Information for Tax Professionals and elsewhere in this manual. You should call your attorney as soon as you discover the breach or security incident.¹⁷³

¹⁶⁸ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

¹⁶⁹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-4>

¹⁷⁰ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷¹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷² <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷³ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

In some states, data thefts must be reported to various authorities—each state has its own unique breach notification requirements. Practitioners can find where to report data security incidents at the state tax level by emailing the Federation of Tax Administrators at statealert@taxadmin.org. You will also need to notify non-tax regulatory entities at the state level—your attorney will have this information, and as part of your incident response plan, you should call your attorney as soon as you become aware of a breach or security incident.¹⁷⁴

Create a data theft recovery plan (incident response plan)¹⁷⁵

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 (within 24 hours).

Contacting the IRS and law enforcement:¹⁷⁶

- Internal Revenue Service. Report client data theft to local IRS Stakeholder Liaisons, who will notify IRS Criminal Investigation and others within the agency on the tax professional’s behalf. Speed is critical. If reported quickly, the IRS can take steps to block fraudulent returns in clients’ names, helping your firm and your clients.
- Federal Bureau of Investigation, local office (if directed).
- Secret Service, local office (if directed).

Contacting states in which the tax professional prepares state returns:¹⁷⁷

- State revenue agencies. Any breach of personal information could have an effect on the victim’s tax accounts with the state revenue agencies as well as the IRS. To help tax professionals find where to report data security incidents at the state level, the Federation of Tax Administrators has created a special email address as a contact point: StateAlert@taxadmin.org.
- State Attorneys General for each state in which the tax professional prepares returns. Most states require that the attorney general be notified of data breaches, so this notification process may involve multiple offices in some locations.
- Additional reporting entities, as required by law, in the applicable states (for example, in New York, this may include the New York Department of Financial Services and the entities noted in the New York SHIELD Law, which include the State Police).¹⁷⁸

¹⁷⁴ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷⁵ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷⁶ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷⁷ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁷⁸ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

Contacting experts:¹⁷⁹

- Security expert. They can help determine the cause and scope of the breach as well as stop the breach and prevent further breaches from occurring -your cybersecurity liability policy may pay for this—check your policy NOW, before any reportable security event occurs!).
- Insurance company. Not only to report the breach, but to check if the insurance policy covers data breach mitigation expenses (Determine in your Security Plan or IRP the entities you will need to contact and the order in which you will contact them—some tax practitioners select either an attorney or their cyber liability insurance carrier /broker as the first entity to contact in the event of a reportable breach).

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—in many jurisdictions, as long as the key has not been lost or stolen, encryption is at least a partial defense for certain reporting requirements—you still must notify regulatory entities, state attorney general, etc. in a timely manner.
- Clients. Consult with your attorney before sending anything to 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.

Remember: IRS toll-free assisters cannot accept third-party notification of tax-related identity theft. Again, preparers should use their local IRS Stakeholder Liaison to report data loss.¹⁸⁰

¹⁷⁹ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

¹⁸⁰ <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-5>

Unit

4

NIST's Small Business Information Security—The Fundamentals

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Explain** the NIST security framework requirements for securing taxpayer data.
- ☐ **Implement** NIST requirements throughout your practice.

In this unit we'll look at NIST's small business-centric framework and observe the consistencies with cybersecurity requirements mandated in the IRS publications of Unit 3.

NIST'S SMALL BUSINESS INFORMATION SECURITY—THE FUNDAMENTALS¹⁸¹

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.¹⁸² This document starts with definitions and a discussion on risk.

¹⁸¹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

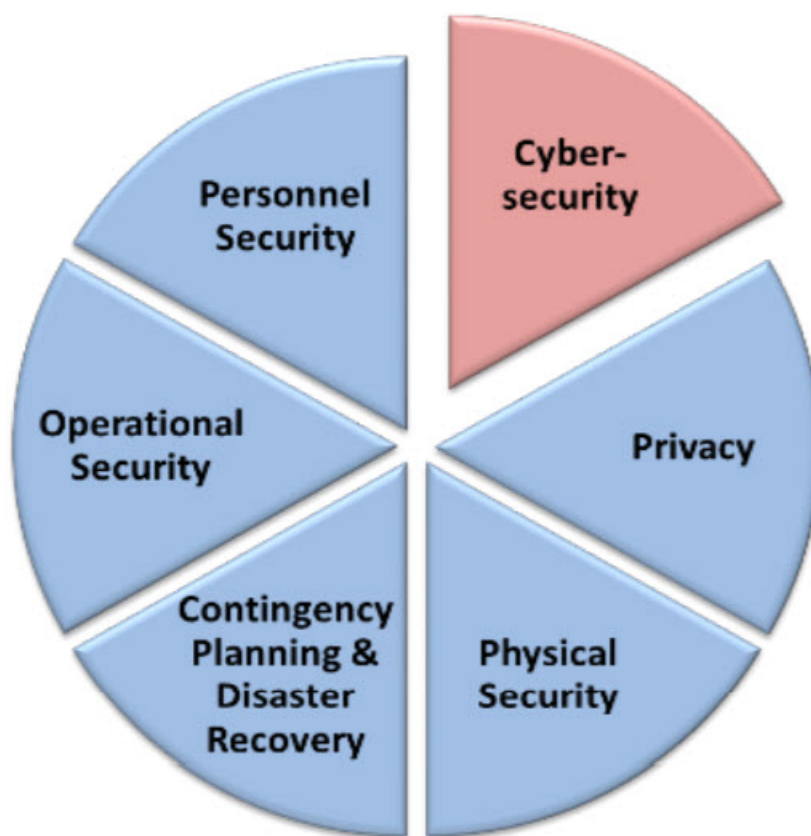
¹⁸² <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Background: What Is Information Security & 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.”¹⁸³

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.”¹⁸⁴

As an integral part of information security, cybersecurity works in conjunction with a variety of other security measures (see following chart). These information security components work together to provide defense against potential threats to your practice’s data.¹⁸⁵



Source: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁸³ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁸⁴ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁸⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

- 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.
- Privacy—protecting personal information.¹⁸⁶

For practitioners, lacking any one of these components diminishes the effectiveness of the others. For example, strong physical security measures mean little if the personnel you hire intend to harm your business (poor personnel security). Strong privacy policies are dependent on cybersecurity practices that protect customer information that is electronically stored.¹⁸⁷

UNDERSTANDING & MANAGING YOUR RISKS¹⁸⁸

Elements of Risk¹⁸⁹

The NIST guidance states that within information security, a threat is anything that might adversely affect the information your practice 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).

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. Vulnerability scans should be performed on a regular basis—the NYDFS Cybersecurity Regulation requires twice per year vulnerability scans and annual penetration testing, along with an annual risk assessment.¹⁹⁰

Likelihood is the chance that a threat will affect your business and helps determine what types of protections to put in place. Likelihood can be thought of as the odds that a threat will occur.

¹⁸⁶ Personal information includes “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.”

¹⁸⁷ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁸⁸ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁸⁹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹⁰ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

The **impact** an event could have depends on the information affected, the business, and the industry. Outcomes can include financial, reputational, market, and regulatory impacts.

Managing Your Risks/Performing a Risk Assessment¹⁹¹

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, changing 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).
- Determine the value of your information.
- Go through each information type you identified and ask these key questions:
 - What would happen to my business if this information was made public?
 - What would happen to my business if this information was incorrect?
 - What would happen to my business if I/my customers couldn't access this information?

These questions relate to confidentiality, integrity, and availability, as discussed in Section 1.1 and help determine the potential impact of an event. Table 1 below shows a template worksheet or spreadsheet you can adapt and use to identify the value of your information. Table 1 also includes some additional, helpful questions to consider what would happen to your business reputation, your productivity, and your legal liabilities.¹⁹²

You may not be able to assign a dollar value amount for many types of information, so instead, consider using a scale of 0 to 3 or “none,” “low,” “moderate,” and “high.”¹⁹³

Using the answers to these questions, rank how critical each type of information is to the continued operations of your business. When calculating an overall ranking or risk score for an information type, either add the values to give a total value or 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.” Information that has a higher score needs to be more protected than information with a low score (higher-rated information

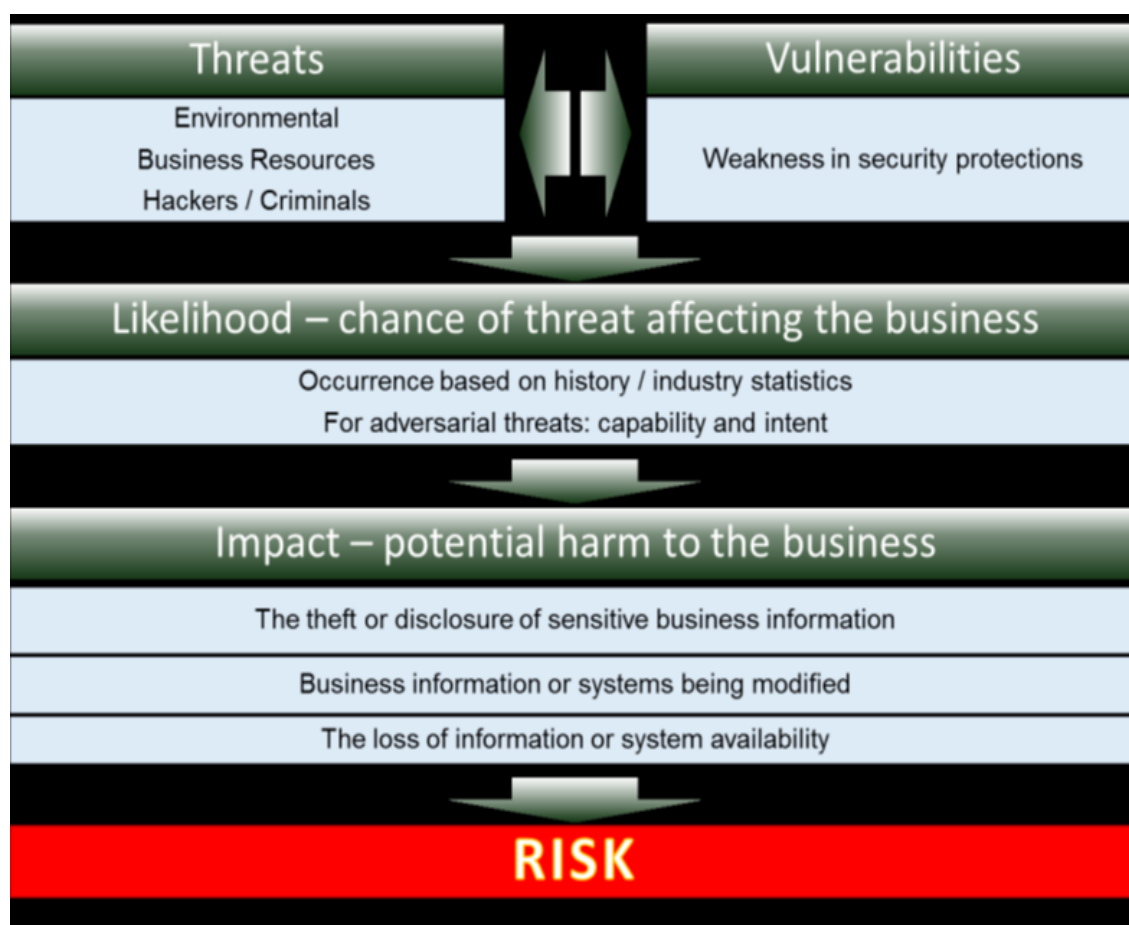
¹⁹¹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹² <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹³ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

types may warrant use of the techniques identified at the end of this publication) of this publication. See Table 1.¹⁹⁴

The relationship between threats, vulnerabilities, impact, and likelihood is as follows:



Source: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹⁴ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Table 1: Identify and Prioritize Information Types

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

Source: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Develop an Inventory¹⁹⁵

Identify what technology comes in contact with the information you listed in Table 1.

Complete Table 2 to include the technology you use to store, access, process, and transmit that information. This can include hardware (e.g., computers) and software applications (e.g., browser email). Make sure to include the make, model, serial numbers, and other identifying information; this information is necessary for identifying the product in case of maintenance, repair, or insurance purposes. Be sure to include locations of the technology.¹⁹⁶

Every information type should have at least one hardware/software technology listed. Where applicable, include technologies outside of your business (e.g., the cloud) and any protection technologies you have in place, such as firewalls.¹⁹⁷

¹⁹⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹⁶ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹⁷ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Evaluate the impact of the information, as decided in Table 1—this will help you determine the most appropriate security controls needed to protect the information. You may choose to add up impact scores for all types of information the product comes in contact with, or only use the highest score. Update this list at least annually.¹⁹⁸

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	<i>Dr. J. Smith's cell phone; Type – Sonic; Version – 9.0 ID – "Police Box"</i>	<i>Mobile T&S Network</i>	<i>Email; Calendar; Customer Contact Information; Photos; Social Media; Locations; Medical Dictionary Application</i>	<i>High</i>
2				
3				
4				
5				

Source: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Understand Your Threats & Vulnerabilities¹⁹⁹

NIST continues with an instruction to regularly review what threats and vulnerabilities your business may face and estimate the likelihood that you will be affected by that threat or vulnerability. This can help you identify specific strategies to protect against that threat or vulnerability.²⁰⁰

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.²⁰¹

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.”²⁰²

¹⁹⁸ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

¹⁹⁹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰⁰ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰¹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰² <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

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.²⁰³

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.²⁰⁴

The information gathered in Tables 1—3 provide the information necessary to identify the areas where you need to focus your information security efforts. 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.²⁰⁵

²⁰³ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰⁴ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

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

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

Source: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Table 4: Prioritize Resolution Action

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

Source: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Safeguarding Your Information²⁰⁶

***Identify*²⁰⁷**

Practitioners should identify and control who has access their business information, including:

- conduct Background Checks—be aware that retaining a report or supporting documentation for this exercise is probably protected by many privacy laws;
- require individual user accounts for each employee based on role; and
- create policies and procedures for information security (include IRC sections as well as privacy of taxpayer data in your WISP and employee handbook).

Protect

According to NIST, the Protect Function supports the ability to limit or contain the impact of a potential information or cybersecurity event, and practitioners should take the following protective actions.

- 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 on a periodic basis (“Patch Tuesday”).

²⁰⁶ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰⁷ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

- Install and activate software and hardware firewalls on all your business networks (Next Generation Firewalls will often include IDS/IPS).
- Secure your wireless access point and networks WPA 2.0.
- Use a VPN; separate the Guest Wi-Fi from the business Wi-Fi.
- 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 and for email messages/attachments, but don't forget/lose your encryption password or key.
- Dispose of old computers and media safely—state laws govern data disposal, so ensure that you remove any data from your equipment before disposal and confirm that you are following all applicable state data disposal requirements.

Employees should be trained 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—acceptable use
- How to work with, process, or handle sensitive/confidential/private taxpayer data, or business information, for example whether or not they can copy or download this data
- What to do in case of an emergency or security incident—they should understand your IRP and their roles in the plan²⁰⁸

Detect²⁰⁹

This section focuses on NIST's detection and monitoring controls.

Practitioners should install and update antivirus, anti-spyware, and other anti-malware programs, with regular periodic updates. Practitioners should also 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.

²⁰⁸ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²⁰⁹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Respond²¹⁰

NIST advises businesses to develop a plan for disasters and information security incidents and to test the plan at least annually. The plan should include the following elements:

- Practitioners should define roles and responsibilities. This includes who makes the decision to initiate recovery procedures and who will be the contact with appropriate law enforcement personnel, as well as who will contact your attorney and your cyber liability insurance representative.
- Define the activities relating to your information and information systems in case of an incident or breach. This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.
- Create a “who to call in case of an incident” list as part of your IRP. This should include how and when to contact your attorney, cyber liability insurance representative, senior executives, emergency personnel, cybersecurity/forensic professionals, service providers/vendors, or other insurance providers. Be sure to include up-to-date and relevant contact information in the plan.
- Many states have breach notification laws which require you to notify clients 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—go over this information with your attorney before a reportable security incident or breach occurs.
- Include when/whether 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—before calling the FBI, contact your attorney and then your cyber liability insurance representative.
- Develop a plan for disasters and information security incidents—at a minimum, draft an IRP and a Business Continuity Plan. NIST advises that 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—more importantly, discuss with your attorney the following: is this incident reportable? How much time do we have to respond? Who do we have to contact? Do we have any defenses?
 - 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. Update the plan annually and include your attorney in all discussions.²¹¹

²¹⁰ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²¹¹ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Recover²¹²

NIST states that the Recover Function helps an organization resume normal operations after an event. To ensure a relatively smooth recovery, be sure to take full backups of important business data/information on a regular basis. It is also a good practice to try accessing the backups to see if they are fully accessible.

Perform a full, encrypted backup of the data on each computer and mobile device used in your business at least once a month (better if done on a daily basis), shortly after a complete virus scan. Store these backups away from your office (cloud or secured encrypted external device) in a protected place so that if something happens to your office, your data is safe. Save a copy of your encryption password or key in a secure location separate from where your backups are stored, and do not forget or lose the password or key.

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, perform adequate due diligence when selecting a Cloud Service Provider. Many have been attacked over the past few years. It is recommended that you encrypt all data prior to storing it in the Cloud. Again, don't lose or forget the encryption key/password.

Test your backups immediately after generating them to ensure that the backup was successful and that you can restore the data if necessary.

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 (ideally daily if possible). 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).

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. Keep in mind that you may want to locate your backed-up data in another part of the United States or outside of the country to minimize the impact of a local disaster.²¹³

²¹² <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²¹³ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

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.²¹⁴

You may want to consider encrypting your backups, but don't lose your decryption key or password!

Make improvements to processes/procedures/technologies²¹⁵

Finally, NIST recommends that practitioners regularly assess their processes, procedures, and technology solutions according to their risks, and to make corrections and improvements as necessary.²¹⁶

As a best practice, practitioners may want to consider conducting or purchasing specific table-top exercises which simulate a major event scenario in order to identify potential weaknesses in current processes, procedures, technology, or personnel readiness. Common scenarios include ransomware, key vendor collapse, and a successful phishing ruse.²¹⁷

²¹⁴ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²¹⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²¹⁶ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

²¹⁷ <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

Unit

5

GLBA/FTC Rules in Detail

LEARNING OBJECTIVES

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Discuss** how the GLBA Privacy and Safeguards (Security) Rules are applicable to tax practitioners and how the FTC enforces compliance with GLBA requirements.
- ☐ **Review** what the FTC has done to enforce compliance with GLBA and what the agency has identified as violations over the past two decades.

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.”²¹⁸

The FTC continues to have enforcement authority. GLBA has delegated its authority to the Federal Trade Commission (FTC) in this area.

There are four GLBA rules covered by FTC regulations:

1. Financial Privacy (Privacy)
2. Safeguards (Security)

²¹⁸ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

3. Red Flags (CPAs received a permanent exemption from this section in 2010)²¹⁹
4. Pretexting (Social Engineering/Phishing)

We will go through the GLBA/FTC Privacy and Security Rules in detail, starting with the Privacy Rule. Be cognizant that IRS confidentiality and/or AICPA confidentiality rules may be more stringent than confidentiality sections of the Privacy Rule.

THE PRIVACY RULE²²⁰

The Privacy Rule, which went into effect in 2000, requires a “financial institution”—this term has a very broad interpretation which includes tax practitioners—to inform customers about its information-sharing practices and allow customers to opt out of having their information shared with certain third parties. CPAs must read this rule within the context of IRS and AICPA regulations which also cover taxpayer nonpublic personal information (NPI) and client confidentiality. These rules are discussed elsewhere in this document.

The Privacy Rule protects a consumer's 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."²²¹

According to the FTC, NPI **is**²²²

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);

And is **not**

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

²¹⁹ CPAs Gain Statutory Exemption from Red Flags Rule, by Matthew C. Lamoreaux, December 21, 2010, <https://www.journalofaccountancy.com/news/2010/dec/20103681.html>

²²⁰ <https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf>

²²¹ 16 CFR Part 313: <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²²² <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

lawfully available to the public; and that the individual can direct that it not be made public **and has not done so**.

The FTC states that 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.²²³

Information in a list form may be NPI, depending on how the list is derived. For 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.²²⁴

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.²²⁵

Examples of NPI (in list form) include a list of a retailer's credit card customers; a list of a payday lender's customers; and a list of auto loan customers merged with list of car magazine subscribers.²²⁶

OBLIGATIONS UNDER THE PRIVACY RULE

Privacy Notices

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.²²⁷ The following five pages show examples of web-facing Privacy Notices and one for a Cookies Policy:

- Deloitte Tax Privacy Notice for the US
- Deloitte Privacy Statement

²²³ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

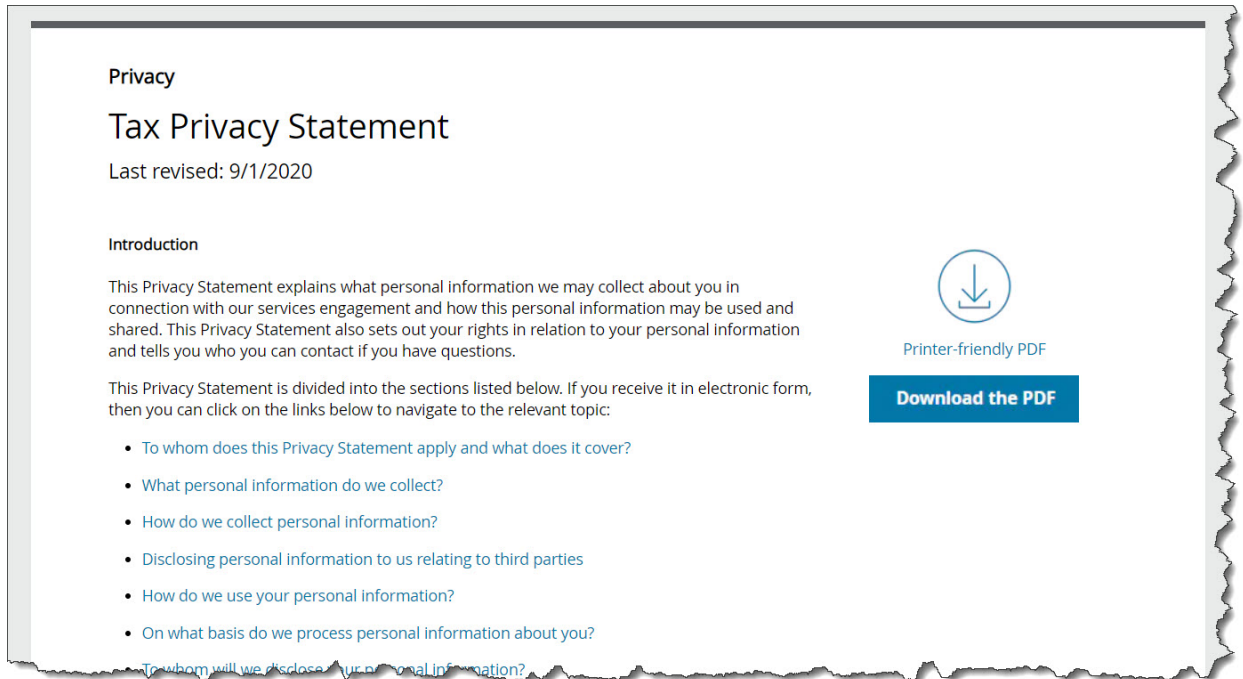
²²⁴ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²²⁵ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

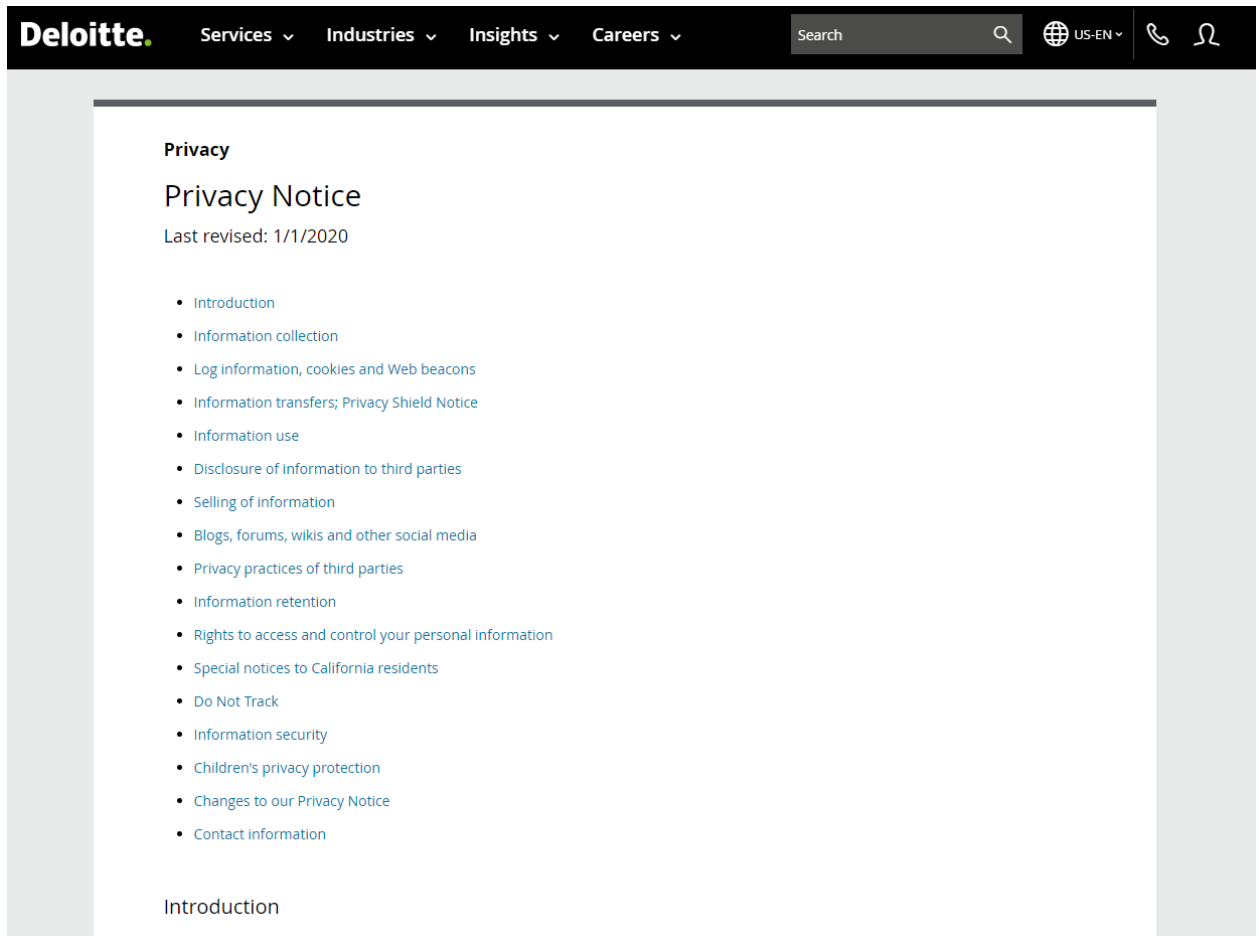
²²⁶ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²²⁷ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

- EY Privacy Statement
- EY Cookie Policy
- H&R Block's Privacy Notice



Source: <https://www2.deloitte.com/us/en/legal/tax-privacy.html>



The screenshot shows the Deloitte website's Privacy Notice page. The header includes the Deloitte logo and navigation links for Services, Industries, Insights, and Careers. A search bar and a language selector (US-EN) are also present. The main content area is titled "Privacy Notice" and "Last revised: 1/1/2020". Below this is a list of links for various privacy topics, including Introduction, Information collection, Log information, cookies and Web beacons, Information transfers, Privacy Shield Notice, Information use, Disclosure of information to third parties, Selling of information, Blogs, forums, wikis and other social media, Privacy practices of third parties, Information retention, Rights to access and control your personal information, Special notices to California residents, Do Not Track, Information security, Children's privacy protection, Changes to our Privacy Notice, and Contact information. The "Introduction" link is highlighted.

Deloitte. Services Industries Insights Careers

Search

US-EN

Privacy

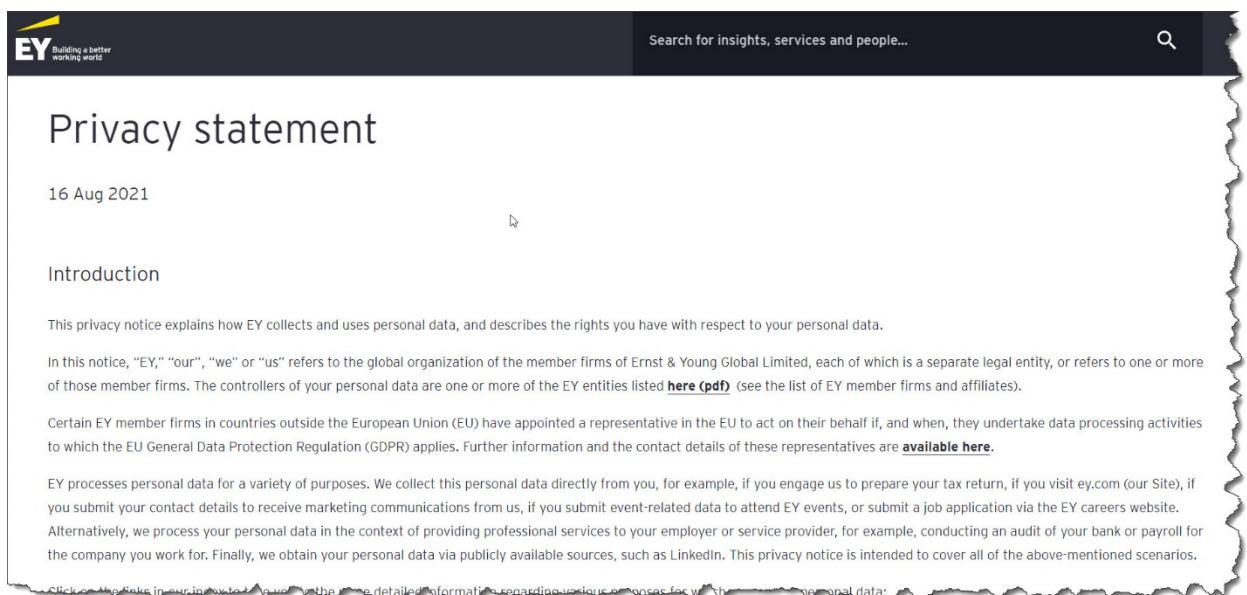
Privacy Notice

Last revised: 1/1/2020

- [Introduction](#)
- [Information collection](#)
- [Log information, cookies and Web beacons](#)
- [Information transfers; Privacy Shield Notice](#)
- [Information use](#)
- [Disclosure of information to third parties](#)
- [Selling of information](#)
- [Blogs, forums, wikis and other social media](#)
- [Privacy practices of third parties](#)
- [Information retention](#)
- [Rights to access and control your personal information](#)
- [Special notices to California residents](#)
- [Do Not Track](#)
- [Information security](#)
- [Children's privacy protection](#)
- [Changes to our Privacy Notice](#)
- [Contact information](#)

[Introduction](#)

Source: <https://www2.deloitte.com/us/en/legal/privacy.html>



The screenshot shows the EY Privacy Statement page. The header includes the EY logo and a search bar. The main content area is titled "Privacy statement" and "16 Aug 2021". Below this is an "Introduction" section. The text explains how EY collects and uses personal data, describes the rights you have with respect to your personal data, and provides information about the EY entities listed in the privacy statement. The text also mentions that EY processes personal data for a variety of purposes, including preparing tax returns, marketing communications, and job applications. The text concludes by stating that this privacy notice is intended to cover all of the above-mentioned scenarios.

EY Building a better working world

Search for insights, services and people...

Privacy statement

16 Aug 2021

Introduction

This privacy notice explains how EY collects and uses personal data, and describes the rights you have with respect to your personal data.

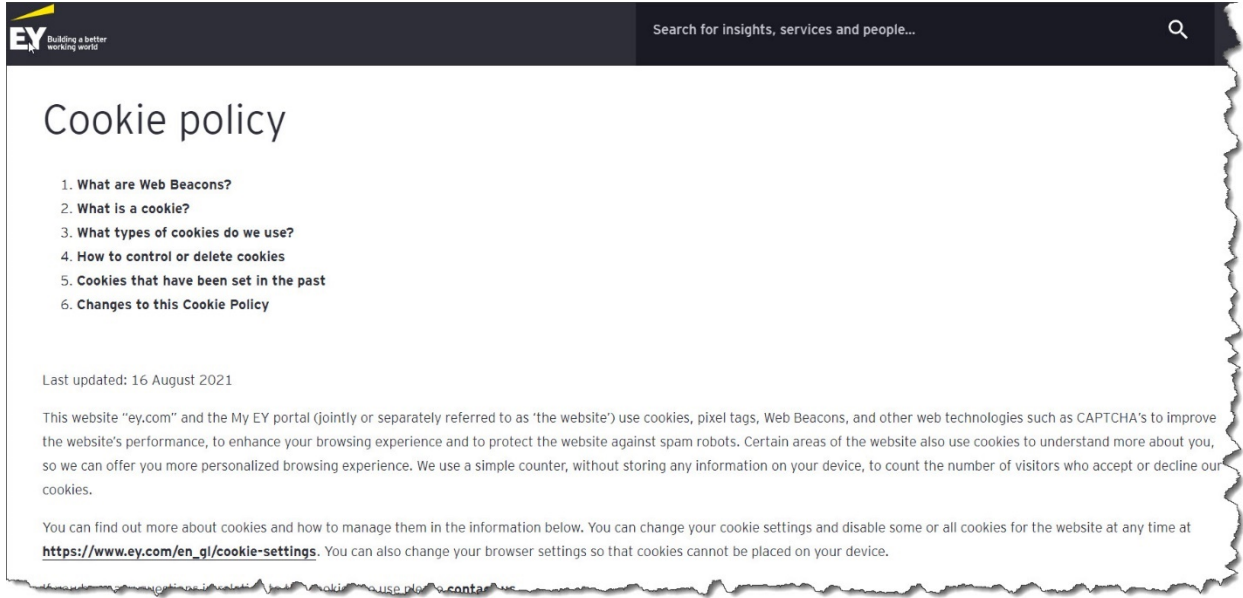
In this notice, "EY," "our", "we" or "us" refers to the global organization of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity, or refers to one or more of those member firms. The controllers of your personal data are one or more of the EY entities listed [here \(pdf\)](#) (see the list of EY member firms and affiliates).

Certain EY member firms in countries outside the European Union (EU) have appointed a representative in the EU to act on their behalf if, and when, they undertake data processing activities to which the EU General Data Protection Regulation (GDPR) applies. Further information and the contact details of these representatives are [available here](#).

EY processes personal data for a variety of purposes. We collect this personal data directly from you, for example, if you engage us to prepare your tax return, if you visit ey.com (our Site), if you submit your contact details to receive marketing communications from us, if you submit event-related data to attend EY events, or submit a job application via the EY careers website. Alternatively, we process your personal data in the context of providing professional services to your employer or service provider, for example, conducting an audit of your bank or payroll for the company you work for. Finally, we obtain your personal data via publicly available sources, such as LinkedIn. This privacy notice is intended to cover all of the above-mentioned scenarios.

Click on the links in our privacy statement to find out the more detailed information regarding unique purposes for which we process your personal data.

EY Privacy Statement: https://www.ey.com/en_us/privacy-statement



EY Cookie Policy: https://www.ey.com/en_us/cookie-policy

H&R BLOCK PRIVACY NOTICE

◀ Back to Free File Program

PRIVACY NOTICE FOR H&R BLOCK'S FREE FILE WEB-BASED AND SOFTWARE-BASED TAX PREPARATION PROGRAMS AND SERVICES

Protecting your privacy is important to us. The following guidelines set forth our general privacy practices and principles that apply to information we collect through our free file web-based and software-based tax preparation programs and related services, which are owned or operated by HRB Digital LLC (collectively, "we," "us," "our,"). These guidelines are based on our business practices, applicable laws and regulations, and our obligations as an industry member of Free File, Inc. (FFI). This privacy notice also details choices available to you regarding the use of, your access to, and how to update and correct your personal information.

Where we collect information on the H&R Block website for other purposes (such as when you locate an H&R Block office online or register a software product with us for warranty purposes, or when you transmit information through our servers), the information that is collected about you will be governed by the "H&R Block Digital Privacy Notice," which can be found at https://www.hrblock.com/universal/digital_online_mobile_privacy_principles.html.

If you enter into another business relationship with us, another H&R Block company, or an H&R Block independently-owned, third-party franchisee, including through our nationwide network of offices, we will make you aware of the privacy practices and principles that apply to that particular business or relationship.

Special Note to Parents: Because of the nature of the services we provide, we do not market our services to children under the age of 13, nor do we knowingly collect information from children under the age of 13.

H&R Block's Privacy Notice: <https://www.hrblock.com/ffa/universal/digital-online-mobile-privacy-principles.html?otppartnerid=180>

Who Gets a Privacy Notice?

Customers get a privacy notice. Whether or not you share customer NPI, you must give all your customers a privacy notice.²²⁸ Under IRC Section 7216, Opt-Out Notices/Options are disallowed.^{229, 230} The "annual notice" requirement does not apply to CPAs (Section 609 of the Financial Services Regulatory Relief Act of 2006).²³¹ The Fair Credit Reporting Act, which is included in the Privacy Rule, is not included in this course.

²²⁸ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²²⁹ <https://www.irs.gov/e-file-providers/section-7216-updated-rules-for-tax-preparers-updated-12-18-2008>

²³⁰ <https://www.irs.gov/tax-professionals/section-7216-frequently-asked-questions>

²³¹ <https://www.govinfo.gov/content/pkg/PLAW-109publ351/pdf/PLAW-109publ351.pdf>

The Contents of the Privacy Notice²³²

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. For example, financial services providers, such as mortgage brokers and insurance companies; or non-financial companies, such as magazine publishers, retailers, direct marketers, and nonprofit organizations. You also may describe categories of other nonaffiliated parties to whom you may disclose NPI in the future.²³³ Categories of information disclosed and to whom under the joint marketing/ service provider exception are in section 313.13 of the Privacy Rule (see "Exceptions").²³⁴

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."²³⁵

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.²³⁶

Your policies and practices with respect to protecting the confidentiality and security of NPI (see "Safeguarding NPI").²³⁷

You only need to address those items listed above that apply to you. For example, if you don't share NPI with affiliates or nonaffiliated third parties except as permitted under sections 313.14 and 313.15, you can provide a simplified notice that: (1) describes your collection of NPI; (2) states that you only disclose NPI to nonaffiliated third parties "as

²³² <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²³³ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²³⁴ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²³⁵ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²³⁶ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²³⁷ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

permitted by law;” and (3) explains how you protect the confidentiality and security of NPI.²³⁸

The privacy notice must be “clear and conspicuous,” whether it is on paper or on a website. It must be reasonably understandable, and designed to call attention to the nature and significance of the information. The notice should use plain language, be easy to read, and be distinctive in appearance. 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.²³⁹

Delivering Privacy Notices²⁴⁰

Practitioners 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.²⁴¹

Exceptions to the Notice & Opt-Out Requirements²⁴²

The section 15 (Section 313.15) 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”).

To take advantage of the section 13 (Section 313.13) exception, you must enter into a contract with those nonaffiliated third parties with whom you share NPI. The agreement must guarantee the confidentiality of the information by prohibiting the third party or

²³⁸ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²³⁹ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴⁰ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴¹ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴² <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

parties from using or disclosing the information for any purpose other than the one for which it was received.²⁴³

LIMITS ON REUSE & REDISCLOSURE OF NPI²⁴⁴

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.²⁴⁵

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.

DISCLOSURE OF ACCOUNT NUMBERS IS PROHIBITED²⁴⁶

The FTC and 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. Note that the sharing of taxpayer PII/personal data may be permitted among several practitioners who are working on the same return or related documentation, but note the additional consent requirements for CPA practitioners performing this activity.²⁴⁷

²⁴³ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴⁴ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴⁵ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴⁶ <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>

²⁴⁷ <https://www.aicpa.org/interestareas/tax/resources/standardsethics/section7216>

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/identityinformationandtools.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

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. As discussed earlier, CPA tax practitioners are considered financial institutions” under GLBA. 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.²⁴⁸

As mentioned earlier, CPA firms are exempted from providing annual privacy notices under section 609 of the Financial Services Regulatory Relief Act of 2006, but note that other privacy laws require covered entities to provide a Privacy Notice (usually a web-facing document with links; see Deloitte web-facing Tax Privacy Notice earlier).

SAFEGUARDS RULE^{249, 250}

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.^{251, 252}

²⁴⁸ Bureau of Consumer Financial Protection 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/>

²⁴⁹ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁵⁰ Taxpayer data, Customer data, and taxpayer/customer information are all used with the same meaning in this chapter.

²⁵¹ Cyber liability: Managing evolving exposures, Stanley Sterna, J.D., and Joseph Wolfe, January 1, 2019, <https://www.journalofaccountancy.com/issues/2019/jan/cyber-liability-exposures.html>

²⁵² 16 C.F.R. §313.1(b).

The Safeguards Rule, which went into effect in 2003, requires financial institutions to develop, implement, and maintain a comprehensive information security program.²⁵³

In addition, the Safeguards Rule, 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.²⁵⁴

The definition of customer information comprises any record containing nonpublic personal information (personally identifiable information and 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),²⁵⁵ about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of tax practitioners or affiliates, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Safeguards Rule and the Privacy Rule use the same definitions of customer and customer relationship.

SECURITY PLAN²⁵⁶

The Safeguards Rule requires tax practitioners to develop and implement 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. You may also want to form a cybersecurity committee comprising two or more persons, including the designated individual.

- Practitioners must also 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. You must perform a periodic risk assessment, ideally on an annual basis.
- Practitioners must design and implement a safeguards program, and regularly monitor and test it.
- Practitioners must select service providers/vendors that can maintain appropriate safeguards—make sure your contract requires your vendors to maintain their own safeguards, and that they oversee their own handling of customer information, especially taxpayer data that you are sharing with them.
- Practitioners must evaluate and adjust the vendor oversight program in light of relevant circumstances, including changes in the vendor firm's business or operations, or the results of security testing and monitoring.²⁵⁷

²⁵³ Safeguards Rule, 16 CFR 314.3(a).

²⁵⁴ Safeguards Rule, 16 CFR 314.3(a).

²⁵⁵ 16 CFR 313.3(n).

²⁵⁶ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁵⁷ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

SECURING INFORMATION²⁵⁸

According to the FTC, 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—perform a data inventory on a regular basis (at least annually) and wipe or destroy unneeded data.²⁵⁹

Depending on the nature of their business operations, firms should consider implementing the following practices:²⁶⁰

- Practitioners should offer cybersecurity training to their employees upon hire and at least annually thereafter. The training should include social engineering and phishing prevention as well as a tabletop exercise.
- From a human resources perspective, practitioners should conduct a background check on prospective hires who will be processing taxpayer data and should also require all employees to sign off/acknowledge the firm's employee handbook or separate document/s relating to confidentiality, security, and protection of taxpayer data that they process or have accessed.
- From an access perspective, practitioners should implement and enforce access policies. Consider limiting taxpayer data access to employees who have a business reason to see it. For example, grant access based on the employee's role.²⁶¹
- Practitioners can control 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.) Current best practices suggest 12 characters or a passphrase of 12 or more characters.²⁶²
- Employees should use password-activated screen savers to lock their computers after a brief period of inactivity and should be trained to lock their devices when leaving their work areas. Best practices suggest that screen settings be set to automatically lockout after a short period of inactivity.²⁶³
- Practitioners should draft and implement policies, procedures, and controls for appropriate use and protection of laptops, and other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, encrypt the hard drives of these devices which contain taxpayer data.²⁶⁴

²⁵⁸ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁵⁹ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶⁰ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶¹ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶² <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶³ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶⁴ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

- Train your employees to take basic steps to maintain the security, confidentiality, and integrity of customer or taxpayer data, including locking rooms and file cabinets where paper records and/or external drives are kept; not sharing or openly posting employee or guest network passwords in work/public areas; encrypting customer or taxpayer data 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 or taxpayer data; and reporting any suspicious attempts to obtain taxpayer or customer information to designated personnel.²⁶⁵
- Practitioners should regularly inform all employees of your practice’s policy—and legal requirements—to keep taxpayer and customer information secure and confidential. For example, consider reminding employees about their responsibility for security in periodic training and within the employee handbook.²⁶⁶
- Develop policies, procedures, and controls for remote employees. For example, consider whether or how employees should be allowed to keep or access customer data at home—best practices would suggest that for most employees, copying and downloading functions should be disabled on their firm-issued devices and that read-only should be the setting for email on both firm-issued and BYOD devices. Also, require employees with BYOD devices to install and update antivirus, operating system updates, and other patches or perform this task centrally with direct corporate access to non-personal areas of BYOD devices.
- Practitioners should implement a progressive system of disciplinary measures for security policy violations, including by immediately deactivating login data and system access, as well as physical access, of terminated employees.

Information Systems²⁶⁷

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Below are some suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:

- Know where taxpayer and customer data is stored and store it securely. Make sure only authorized employees have access, and ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
- Store paper records and external hard drives in a room or cabinet that is locked when unattended.
- When taxpayer or customer data is stored on a server or other computer, ensure that the data is accessible only with a strong password (best practices suggest a 12-character password or a longer passphrase) and is kept in a physically secure area.

²⁶⁵ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶⁶ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶⁷ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

- Where possible, avoid storing taxpayer or customer data on a computer with an Internet connection—it is better to use an encrypted external hard drive or to upload through encryption to the cloud.
- Maintain secure encrypted backup records (but don't lose or forget the key/password) and keep archived data secure by storing it off-line/encrypted and in a physically secure area or in the cloud.
- Maintain a physical inventory of your practice's firm-issued workstations and mobile devices and any other equipment on which taxpayer or customer data may be accessed (including BYOD, if applicable).²⁶⁸

Practitioners should take steps to ensure the secure transmission of customer information. For example:²⁶⁹

- When you transmit taxpayer data, 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 taxpayers or 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 (use forced TLS)—a portal with MFA access is a more secure option;
- Dispose of taxpayer and customer data in a secure way and, where applicable, consistent with the FTC's Disposal Rule and applicable state data disposal laws;
- Consider designating or hiring a records retention manager to supervise the disposal of records containing taxpayer or 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;²⁷⁰
- Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed; and
- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, mobile devices, or any other electronic media or hardware containing customer information—don't forget cloud data disposal.²⁷¹ Also, ensure that you comply with all requirements of the FTC Disposal Rule.

²⁶⁸ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁶⁹ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷⁰ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷¹ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

FTC Disposal Rule:²⁷² Proper Disposal of Consumer Information (See Also State Data Disposal Laws)

- a. Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.
- b. Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with the rule in this part.
 - 1. Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.
 - 2. Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
 - 3. After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.
 - 4. For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (b)(1) and (2) of this section.
 - 5. For persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314 (Safeguards Rule), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.

²⁷² 16 CFR 682.3.

Detecting & Managing System Failures²⁷³

Effective security management requires your practice to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:²⁷⁴

- Practitioners should monitor the websites of software vendors and reading relevant industry publications for news about emerging threats and available defenses.
- Practitioners should maintain up-to-date and appropriate programs and controls to prevent unauthorized access to taxpayer information, including installing patches and updates that resolve software vulnerabilities, installing antivirus and anti-spyware with automated updates; maintaining up-to-date firewalls, ensuring that unused ports are closed; and informing employees about any emerging security risks or possible breaches.²⁷⁵
- Practitioners should also implement appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information, including maintaining logs of network activity and monitoring them for signs of unauthorized access to taxpayer information; using an intrusion detection system with automated alerts (but be aware that there may be many false positive alerts generated); monitoring 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 inserting a dummy account into each of your customer lists and monitoring the account to detect any unauthorized contacts or charges.²⁷⁶
- Practitioners should take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If you become aware of a reportable breach or security incident, one of the first actions you should take to contact your attorney to confirm if a breach notification is required under applicable state, federal, or non-U.S. law(s). Other steps to take include the following, which should already be included in your IRP:²⁷⁷
 - 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.
 - If feasible and appropriate, bring in security professionals to help assess the breach as soon as possible—after contacting your attorney, you may want to inform your cybersecurity insurance representative, your forensic expert, and anyone else included in your Incident Response Plan.

²⁷³ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷⁴ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷⁵ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷⁶ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷⁷ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

- Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach (but only after speaking with your attorney who will determine who to notify and when to carry out the notice.²⁷⁸

Safeguards Rule Update

On October 27, 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.²⁷⁹ 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.

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.

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.

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.

START WITH SECURITY: A GUIDE FOR BUSINESS—LESSONS LEARNED FROM FTC CASES²⁸⁰

²⁷⁸ <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>

²⁷⁹ <https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial>

²⁸⁰ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

This document (Federal Trade Commission, 2015) uses actual FTC data security settlements as examples of privacy dos and don'ts. The following is an outline of these recommendations:

1. **Start with security.**²⁸¹ Practitioners should factor security into the decision making in every department of your business, including HR, sales, accounting, information technology, operations, and legal. Practitioners should also implement data collection, retention, and use policies (have a rationale/legitimate business need—statutory requirement/best practices, etc.) and should not collect personal information that is not absolutely needed—very little, if any taxpayer data should be retained indefinitely.
2. **Control access to data sensibly.**²⁸² Practitioners must put controls in place to make sure employees have access only on a need-to-know basis and should consider network access controls that include separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases.

Practitioners should store paper files, external drives, disks, etc., in a locked file cabinet and should restrict access to sensitive data. Also, providers should limit administrative access (also known as admin access, which allows a user to make system-wide changes to your system) to the employees tasked to do that job.

3. **Require secure passwords and authentication.**²⁸³ Practitioners should insist on complex and unique passwords, store passwords securely, use maximum unsuccessful attempt lockouts (increases security against brute force attacks), and protect against authentication bypass—test for common vulnerabilities.
4. **Store sensitive personal information securely and protect it during transmission.**²⁸⁴ Practitioners need to keep sensitive information secure throughout its lifecycle (encrypt data at rest, in transit, and in use), use industry-tested and accepted methods (e.g., PCI-DSS standard, NIST, etc.), and should ensure proper configuration—SSL used (TLS version 1.0 or higher is preferred).
5. **Segment your network and monitor who's trying to get in and out.**²⁸⁵ Practitioners should segment the network (split the network into subnetworks, which limits internetwork communication, and may result in a dead end for a hacker who gains access) as well as monitor activity on the network.
6. **Secure remote access to your network.**²⁸⁶ It is imperative for practitioners to ensure endpoint or extended endpoint security (antivirus, and other solutions such as Endpoint Detection and Response, URL filtering, etc.)²⁸⁷ and to put sensible access limits in place (security software such as AlertLogic can help in this area).

²⁸¹ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁸² <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁸³ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁸⁴ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁸⁵ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁸⁶ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁸⁷ <https://solutionsreview.com/endpoint-security/the-top-11-types-of-endpoint-security-for-enterprises/>, The Top 11 Types of Endpoint Security for Enterprises, May 24, 2019, by Ben Canner.

7. **Apply sound security practices when developing new products.**²⁸⁸ If practitioners employ developers to create new or improved software or proprietary products, train them in secure coding. Practitioners should also follow platform guidelines for security such as not disabling recommended security settings, and providers should verify that privacy and security features work. Practitioners should also test for common vulnerabilities—look out for known vulnerabilities (OWASP)²⁸⁹.
8. **Make sure your service providers implement reasonable security measures.**²⁹⁰ Practitioners should include all security requirements in their vendor contracts and should also verify compliance with evidence (contractual language, SOC 2 reports).
9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**²⁹¹ Practitioners must update and patch third-party software on a periodic basis and must quickly respond to credible security warnings.
10. **Secure paper, physical media, and devices.**²⁹² Practitioners must securely store sensitive files, protect devices that process personal information, keep safety standards in place when data is en route (in transit), and dispose of sensitive data securely and in compliance with applicable state data disposal laws.

²⁸⁸ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

²⁸⁹ <https://www.cloudflare.com/learning/security/threats/owasp-top-10/>, What is OWASP? What Are the OWASP Top 10?, Cloudflare, 2019.

²⁹⁰ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁹¹ <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

²⁹² <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

Unit 6

Confidentiality of Client Tax Data

LEARNING OBJECTIVE

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Describe** the basic relevant laws and professional standards that apply to tax client confidentiality.

CONFIDENTIALITY RESTRICTIONS

Generally, a practitioner is prohibited from disclosing client taxpayer data without client consent. Applicable 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).

Third-Party Disclosure

IRC section 7216 prohibits a CPA from disclosing a client's tax information to a third party without the written consent of the taxpayer. The consent should not be stale.

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.²⁹³

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.²⁹⁴

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. Reg. §301.7216-2(d)(1) without

²⁹³ <https://www.cpajournal.com/2017/03/20/applying-aicpas-professional-standards-tax-practice/>

²⁹⁴ <https://www.cpajournal.com/2017/03/20/applying-aicpas-professional-standards-tax-practice/>

obtaining the taxpayer's consent. For 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.²⁹⁵

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.²⁹⁶

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.²⁹⁷

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.²⁹⁸

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.²⁹⁹

²⁹⁵ A Provider, including an ERO, may disclose tax return information to other Providers relating to e-filing a tax return under Treas. Reg. §301.7216-2(d)(1) without obtaining the taxpayer's consent. For 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.

²⁹⁶ <https://www.cpajournal.com/2017/03/20/applying-aicpas-professional-standards-tax-practice/>

²⁹⁷ <https://www.cpajournal.com/2017/03/20/applying-aicpas-professional-standards-tax-practice/>

²⁹⁸ <https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>

²⁹⁹ <https://www.aicpa.org/interestareas/tax/resources/standardsethics/section7216>

Consent Forms³⁰⁰

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: AICPA Code of Professional Conduct, Section 1.700.001

CPA practitioners must also consider these items as well with taxpayer confidentiality situations, including during reportable breach/security incident occurrences:³⁰¹

- 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"
 - 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"

³⁰⁰ <https://www.aicpa.org/interestareas/tax/resources/standardsethics/section7216>

³⁰¹ <https://www.journalofaccountancy.com/issues/2015/mar/aicpa-confidentiality-rule.html>

- 1.700.080, “Disclosing Client Information in Director Positions”
- 1.700.090, “Disclosing Client Names”
- 1.700.100, “Disclosing Confidential Client Information as a Result of a Subpoena or Summons”

Unit

7

IRS Instructions for Reporting Website Security Incidents & Identity Theft

LEARNING OBJECTIVE

When you have completed this unit, you will be able to accomplish the following:

- ☐ **Report** website security incidents/breaches to the IRS and state tax authorities.

Keep in mind that you will probably be required to report security incidents or breaches to state and privacy and other regulatory bodies in addition to the IRS.

Confirm your specific reporting requirements with your attorney on a periodic basis as laws in this area are constantly evolving.

For example, a security incident (let's say an unsuccessful attempt to access the personal data of your 500 New York state taxpayer clients that was discovered by your cloud vendor) may, under certain conditions, 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;
- within 24 hours (IRS deadline) to the New York City Tax authorities;
- within 10 days, under the New York SHIELD Act, to the New York Attorney General, Department of State, and State Police.

For IRS reporting: the IRS has specific detailed requirements it expects to see when a breach or security incident is reported to the agency. These requirements are listed below;^{302, 303}

- 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:
 - Date and time of the incident
 - Date and time the incident was discovered
 - Source of the incident
 - Method of detection
 - Detail description of the incident
 - Why should the incident be of concern
 - Corrective actions planned or taken
 - Whether taxpayer information was disclosed (Y/N only, do not include taxpayer information)
 - Number of taxpayers impacted
 - Regular business hours contact name, phone number, and email address
 - After-hours contact name, phone number, and email address
 - Provider’s EFIN
 - 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.”

³⁰² Instructions for Reporting Website Security Incidents, <https://www.irs.gov/e-file-providers/instructions-for-reporting-web-site-security-incidents-updated-10-02-08>, last updated October 8, 2019.

³⁰³ <https://www.irs.gov/pub/irs-pdf/p1075.pdf>, Section 10.1, p. 120-122.

[Home](#) / [Tax Pros](#) / [Modernized e-File](#) / [Instructions for Reporting Security Incidents](#)

Instructions for Reporting Security Incidents

Enrolled Agents

Annual Filing Season Program Participants

Enrolled Retirement Plan Agents

Certified Professional Employer Organization (CPEO)

Enrolled Actuaries

E-File Providers

Modernized e-File

Become an Authorized e-file Provider

Authorized IRS e-file Provider
Locator Service for Tax Professionals

Quick Alerts

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**.

Source: Instructions for Reporting Security Incidents | Internal Revenue Service (irs.gov)

Ensure that you have read and understand the latest updated IRS and other applicable reporting requirements and that you have consulted your attorney for confirmation—these requirements should be included in your IRP and updated as necessary:

- <https://www.irs.gov/e-file-providers/instructions-for-reporting-web-site-security-incidents-updated-10-02-08>. In addition, practitioners may also wish to call their local TIGTA field office/the TIGTA Hotline within the 24 hour reporting period—confirm with your attorney first (see following instructions):

10.0 Reporting Improper Inspections or Disclosures**10.1 General**

Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information must contact the office of the appropriate special agent-in-charge, TIGTA immediately, but no later than 24 hours after identification of a possible issue involving FTI. Call the local TIGTA Field Division Office first.

Table 11 – TIGTA Field Division Contact Information

Field Division	Field Division Service Locations	Telephone
Atlanta	Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, Puerto Rico, and U.S. Virgin Islands	(470) 639-3792
Mid-States	Arkansas, Illinois, Iowa, Kansas, Louisiana, Michigan, Minnesota, Mississippi, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin, Northern Ohio, Oklahoma, Texas, Louisiana, Kansas, Missouri, Nebraska	(713) 209-3711
Denver	Alaska, Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Oregon, Utah, Washington, and Wyoming	(801) 620-7734
New York	Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont	(917) 408-5640
San Francisco	California, Hawaii, Guam, American Samoa, Commonwealth of Northern Mariana Islands, Trust Territory of the Pacific Islands	(213) 576-4147
Washington	Delaware, Indiana, Kentucky, Martinsburg Computing Center, Maryland, New Jersey, Pennsylvania, Southern Ohio, Virginia, West Virginia, Washington, DC	(215) 861-1003
Electronic Crimes & Intelligence Division	Any agency reporting a cyber-incident such as data breach may report directly to this division	(240) 613-5230 cybercrimes@tigta.treas.gov

Source: Contact Treasury Inspector General for Tax Administration | Internal Revenue Service (irs.gov)

If unable to contact the local TIGTA Field Division, contact the Hotline Number.

Hotline Number: 800-589-3718

TIGTA Homepage: <https://www.treasury.gov/tigta>

Mailing Address: Treasury Inspector General for Tax Administration
Ben Franklin Station
P.O. Box 589
Washington, DC 20044-0589

10.2 Office of Safeguards Notification Process

Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information
- Date and time the incident occurred
- Date and time the incident was discovered
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred
- IT involved (e.g., laptop, server, mainframe)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. Do not include any FTI in the data incident report.

Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

For reporting identity theft, follow the instructions found in the following identity theft affidavit reporting links:

- <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>

NOTES

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>, Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns (Rev. 11-2020)
- <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>
- <https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1>
- <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>
- <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. 11-2020)
- 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
- 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 November 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/>

Take Advantage of Diversified Learning Solutions

We are a leading provider of continuing professional education (CPE) courses to Fortune 500 companies across the globe, CPA firms of all sizes, and state CPA societies across the country, as well as CPA associations and other financial organizations. Our efficient and flexible approach offers an array of customized cutting-edge content to meet your needs and satisfy the priorities of your business. Select from live classes, live webinars, conferences, or online training, including Nano courses, based on your preferred method of learning.

Meet your CPE requirements, increase productivity, and stay up-to-date with relevant industry trends and mandatory regulations with collaborative live or online learning.

Live Training Topics	Online Training Topics
Accounting and Auditing	Accounting and Auditing
Employee Benefit Plans	Business Law
Ethics	Business Management and Organization
Information Technology	Economics
Governmental and Not-For-Profit	Ethics
Non-Technical (including Professional Development)	Finance
Tax	Information Technology
	Management Services and Decision Making
	Personal and Professional Development
	Tax

“We have enjoyed [your] programs and have found the content to be an excellent learning tool, not only for current accounting and management issues, but also how these issues apply to our company and affect how our business is managed.”

—Debbie Y.

Unauthorized reproduction or resale of this product is in direct violation of global copyright laws.

Reproduced by permission from Kaplan.



© 2022 Kaplan, Inc. All Rights Reserved.