THE PROFESSIONAL TAX RETURN PREPARE - LEGAL AND ETHICAL DUTIES TO RECOGNIZE CYBERSECURITY THREATS AND HOW TO RESOLVE THEM

By Mary E. Vandenack

Vandenack Weaver LLC
402.504.1300
VWTlawyers.com

PRESENTER: MARY E. VANDENACK

- **Mary E. Vandenack, J.D., ACTEC, CAP®, COLPM®, Accredited Estate Planner® (Distinguished) Nominee** is CEO, founding and managing member of **Vandenack Weaver LLC** in Omaha, Nebraska. Mary is a highly regarded practitioner in the areas of tax, trusts and estates, private wealth planning, asset protection planning, executive compensation, business and business succession planning, tax dispute resolution, and tax-exempt entities. Mary also has expertise in mental health law and professional licensing. Mary's practice serves businesses and business owners, executives, real estate developers and investors, health care providers, companies in the financial industry, and tax-exempt organizations. Mary is a member of the American Bar Association Real Property Trust and Estate Section where she serves on the Planning Committee and Council. Mary is a member of the American Bar Association Law Practice Division where she currently serves as Vice Chair. Mary has been named to ABA LTRC Distinguished Women of Legal Tech, received the James Keane Award for e-lawyering, and serves on ABA Standing Committee on Information and Technology Systems. Mary is a frequent writer and speaker on tax, benefits, asset protection planning, and estate planning topics as well as on practice management topics including improving the delivery of legal services, technology in the practice of law and process automation. At conferences, Mary will also often teach a yoga or mindfulness class. Mary hosts a podcast: Legal Visionaries. https://maryvandenack.com/podcast/

CYBERSECURITY THREATS - OBJECTIVES

- Understand the requirements in Publication 5708.
- Understand how to prepare a Written Information Security Plan.
- Understand the Gramm-Leach-Biley Act requiring protection of customer data. Tax and accounting professionals are considered financial institutions for this purpose regardless of size.

CYBER SECURITY THREATS

WHAT IS CYBERSECURITY?

- Protection of Technology Tools from unauthorized access or criminal use and ensuring confidentiality, integrity and availability of information.
- Protecting Devices
- Protecting Networks
- Protecting Data

KEY COMPONENTS OF CYBERSECURITY

- Information Security – protecting data
- Network Security – protecting infrastructure and communication channels
- Endpoint Security – securing individual devices
- Application Security – ensuring software applications can resist attacks
- Cloud Security – Is cloud-based infrastructure secure?
- Identify and Access Management – Verification and authentication of users
- Threat Intelligence – Being aware of emerging threats
- Incident Response and Recovery – Preparation for and planned response to incidents

POLICIES AND TRAINING

- Establish and Enforce cybersecurity policies.
- Security Awareness and Training
  - Educate employees. Users are often the weakest link (using shadow IT, using work email for personal items).
  - Training should occur regularly rather than once a year. Threats change constantly and rapidly.

SOME CYBERSECURITY TERMS

- Cyberattack – A cyberattack is an attempt to gain unauthorized access to a computer system, network, or data.
- Hacker – This is a person who exploits weaknesses in computer systems and software.
- Malicious Code – Malicious code is unwanted files or programs that can cause harm to your system (viruses, worms, trojan horses)
- Vulnerabilities – Vulnerabilities may include flaws in hardware, software, or firmware.
- Botnet – Botnet refers to a network of compromised computers.

WHY IS CYBERSECURITY IMPORTANT FOR TAX PREPARERS?

- The use of tools that facilitate contactless tax preparation have become normal!

- Criminals have long targeted taxpayers.
  - Phishing
  - Smishing
  - Vishing
  - QR-ishing
  - Social Engineering (using any of the above and/or social media)
  - Ransomware

- Tax returns are a target because of the sheer volume of sensitive financial information and personal data.

WHAT IS PHISHING?

- Phishing – An email is sent from a seemingly reputable company seeking to induce individuals to reveal personal information such as passwords and credit card companies.
- Examples: Fake Invoice; Email account upgrade; Advance-fee; Paypal; google docs; dropbox scam.
- What To Look For: Requests for sensitive information, unexpected emails, suspicious attachments, too good to be true.
- What Happens if you click the link? Malware may be downloaded to spy.
- Strategy: Never provide personal information to an unsolicited request. Use email filtering.

RECENT EXAMPLE OF PHISHING

From: Megan Gumbel <megan.gumbel@connectshows.com>
Sent: Wednesday, September 27, 2023 10:56 AM
To: Mary Vandenack <mvandenack@vwtlawyers.com>
Subject: Home Care - 2023

Hi Mary,

I'm writing to check if you would be interested in acquiring verified contact details of "**Home Care**" across the global?

We can assist you with verified contact details of-

Assisted Living and Senior Care Providers

Retirement Community Centers

Long-Term, Home Health Care Providers

Hospice Providers

Geriatric Medicine Specialists

HME/DME Providers

Let me know your target criteria - target industry/job titles/Specialties, so that I can revert with "counts, pricing & few samples" for the same.

Regards,

Megan Gumbel | Campaign Executive

WHAT IS SMISHING?

- Smishing – A text message is sent from a seemingly reputable company seeking to induce individuals to reveal personal information such as passwords and credit card companies.
- Example: Account verification scams – there is usually a warning of unauthorized activity.
- What To Look For: Text is from a strange phone number. Text claims to be from a company you know and trust. Urgency is conveyed. There may be request for money or information.
- What Happens if you click the link? Your phone may be subject to security threats.
- Strategy: Never respond to texts from unknown numbers. Keep your phone operating system up to date.

WHAT IS VISHING?

- Vishing – A phone call is made from a seemingly reputable company seeking to induce individuals to reveal personal information such as bank information and credit card information.
- Example: Cyber criminal calls and appeals to victim's human instincts of trust, fear, greed and desire to help. Criminal may ask for bank account information, credit card details, mailing address. Criminal may request a funds transfer or emailing of confidential documents. Caller may pretend to be a government representative, tech support, telemarketing or banker.
- What To Look For: Call is from a strange phone number. Call claims to be from a company you know and trust. Urgency is conveyed. There may be request for money or information.
- Strategy: Pay close attention to any caller. Do not answer calls from unknown numbers. Never provide personal information to an unsolicited caller. Register your phone number with the Do Not Call Registry.

WHAT IS QR-ISHING?

- QR-ishing – Phone users tend to scan QR codes for a variety of reasons. QR-ishing exploits this tendency.
- Example: Attacker may leave flyers at a bus stop or on a table at a restaurant or coffee shop. When person scans the QR code, victim is tricked into sharing sensitive information.
- What To Look For: QR codes on discount vouchers. A transparent sheath of a scam QR code may be pasted over a legitimate QR code. Look carefully.
- Strategy: Consider blocking Camera Access to your phone to avoid automatic scanning. Do not open shortened URLs. Install security applications on your mobile device. Avoid QR codes.

SOCIAL ENGINEERING

- Social engineering is an attempt to deceive a victim and obtain control over a computer system or steal personal and financial information. Social engineering may use phishing and other strategies.
- Hackers recently breached MGM, Caesars, and three other companies. Hacking was accomplished via social engineering. Hackers impersonated firm employees and convinced the technology helpdesk to provide them duplicate access.
- The hack was accomplished by hacking group ALPHV, who posted about the hack on its website and warned MGM of further attacks if MGM doesn't make a deal.
- Watch out for unexpected emails, phone calls, and voice or text messages.

TECHNOLOGY CRIME STATISTICS

- Every day, about 7 million data records are lost or stolen.
  - 72% of breaches are done by a malicious outsider.
  - 18% are result of accidental loss.
  - 9% are result of malicious insider.
- The FBI's Internet Crime Complaint Center in 2022 received 800,944 complaints. In 2017 there were only 301,850 malicious incidents, so in 5 years it almost tripled!
- The potential total loss has grown from $6.9 billion in 2021 to more than $10.2 billion in 2022. This was only $1.4 billion in 2017.
- The chance of arresting a cybercriminal remains very low.

2023 TAX SEASON

- IRS filters flagged approximately 1.1 million tax returns for identity theft. Total value was approximately $6.3 billion.

- IBM’s Cost of a Data Breach Report 2022 reported that 83% of organizations studied had experienced more than one data breach.

PRIORITIZE CYBERSECURITY

DATA SECURITY MUST BE A HIGH PRIORITY

- Data must be secured at multiple points.
  - In transit
    - File sharing
    - Lawyer client communications
  - While Stored
    - Client server or cloud storage
    - Copies with service providers and experts
  - Data loss issues can result from accidental deletion, hardware failure or issues related to data migration
- An excellent resource: https://lawyerist.com/podcast/law-firm-data-security-with-sharon-nelson-and-john-simek/

CYBER ATTACKS ARE EXPENSIVE

- Costs for forensic discovery, remediation, determination of exfiltration of data, reporting requirements and outside counsel to protect litigation exposure can run between $70,000 and $300,000.
- State and federal reporting and credit monitoring requirements can add additional significant expense if you are breached.
- Breaches may use ransomware (extortion). This is software that denies you access to your system until you pay ransom.
- A breach is also harmful to your reputation, which is costly in ways that are difficult to count.
- Purchase cyber liability insurance.

ORGANIZATIONAL APPROACH

- Make it difficult for scammers to reach organizational users.
  - Anti-spoofing controls
  - Be aware of information that is available to attackers. Consider social media.
  - Filter or block incoming emails.
- Educate your users on how to identify and report suspected emails.
  - Encourage users to seek help rather than hiding an issue for fear of feeling stupid.
- Protect organization from affects of undetected phishing emails.
  - Resistant authentication processes.
  - Use proxy server and up to date browser.
  - Protect devices.
- Respond quickly to incidents.
  - Define and rehearse incident response plan.

ORGANIZATIONAL APPROACH (cont)

- Give due attention to social media. Hackers will review social media to get employee names and take on their identity. Hackers will also hack social media account to obtain information about account holder and contacts.

- Have points of contact for each area of risk and a process to manage the points of contact.

GRAMM-LEACH-BILEY ACT

GRAMM-LEACH-BILEY ACT (GLB)

- This act requires financial institutions to protect consumer data.
- Tax and accounting professionals are considered financial institutions for this purpose.
- Federal Trade Commission (FTC) is responsible for enforcement of GLB.
- FTC has issued Safeguards Rule.
- Rule requires that all paid tax return preparers create AND implement a Written Information Security Plan

IRS Publication 4557 Safeguarding Taxpayer Data: A Guide For Your Business

Vandenack Weaver LLC
402.504.1300
VWTlawyers.com

INTRODUCTION

- If you are ever sued over a data breach, you are precluded from claiming lack of awareness.
- Information and requirements are available in publicly available IRS publications.
- The rules apply to CPA firms AND law firms that prepare gift and estate tax returns, trust companies that prepare trust income tax returns, and perhaps even many financial planning firms as the scope of their work expands.
- Data theft against tax professionals is on the rise.
- Addressing data security is an essential step for the largest firms and firms of all sizes including solo practitioners.
- The IRS recommends that tax preparers hire data security experts, buy cyber security insurance, and educate their staff.
- Tax preparers must create written information security plans to protect client data.

SIX MUST DO'S

- Install anti-malware/anti-virus security software on all devices (including laptops, routers, tablets and phones).
- Ensure software (especially anti-virus and anti-malware), firmware, and operating systems are consistently updated.
- Use long and different passwords for each account. Change the suggested password on any connected device to one of your own.
- Do not click email links unless you're confident of the source.
- Train employees on security practices.
- Have a plan **Written Information Security Plan (WISP)**. See Small Business Information Security - The Fundamentals by the National Institute of Standards and Technology.

OTHER BASIC STEPS

- Learn to recognize the various scams.
- Once you have a written plan, **communicate it**. Update it. Train others about the plan. That is, don't just create it and save it and move on. Make the plan a living tool.
- Encrypt all sensitive files and emails.
- Backup sensitive data to a safe and secure external source. Device should not be connected fulltime to network.
- Wipe clean or destroy old computer hard drives.
- Withdraw from any outstanding authorizations (e.g., power of attorney for tax information) for taxpayers who are no longer clients. You can get a list of all of your appointments from the IRS.
- Report suspected data theft or loss to the IRS immediately.

USE SECURITY SOFTWARE

- THIS IS FUNDAMENTAL!
- Anti-virus prevents malware from causing damage to a computer.
- Anti-spyware prevents unauthorized software from stealing information on your computer.
- A firewall blocks unauthorized access to your system.
- Drive encryption protects information from being read if a device is lost or stolen.
- Whatever you use must be updated regularly.

OTHER STEPS

- Use multi-factor authentication.
- Secure your wireless network.
  - Use a strong unique password for the administrator.
  - Use a name for your router that is not identifiable (e.g., don't call it Tina Tax Saving Service, LLC).
- Protect stored client data.
  - Backup data to secure cloud storage. Know what is being backed up and where.
  - Use drive encryption.
  - Don't attach USB devices with client data to public computers.
- Exercise extreme care in using "free" software.
- Use separate personal and business email accounts. Do you consistently do this?

OTHER STEPS (cont.)

- Remove client files for clients who are deceased or have left your firm. The last thing you want to do is to notify someone of a data breach who is no longer a client of the firm.
- Limit access to taxpayer data to those who need to know. Secure files within the firm to limit access and exposure.
- Make a final review of all return information – especially direct deposit information – prior to e-filing.
- Check e-file applications and PTIN accounts weekly for total returns filed using EFINs and PTINs. Deactivate unused EFINs.
- Do not install unnecessary software.
- Address Shadow IT.

PASSWORD CREATION

- Eight characters is recommended. More is advisable.
- Combine letters, numbers and symbols.
- Don’t use a password that includes information about you that is readily available on your website, social media or on the internet. Google me for example. Sadly, my name isn’t John Smith and I’m easy to find.
- Don’t re-use passwords and don’t simply change one digit.
- Use a password manager.

INTERNET SAFETY

- Look for s in https connections. S stands for secure.
- Do not use public wifi. Consider a mobile secure hotspot. You can always get a second phone with 5G and use that as a redundant system and hotspot.
- Disable password storage. Use a password manager. Then, you have security and you only have to remember one password.
- Enable browser pop-up blocker.
- Be aware if your home page changes when the change was not initiated by you.
- Download files only from known websites or applications.

REPORT DATA BREACHES

- Report data breaches to:
  - IRS. Specifically report to IRS Stakeholder Liaison. https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts
  - FBI.
  - Police (file a police report).
  - States in which you file returns see StateAlert@taxadmin.org
  - State attorney general for states in which you prepare returns.
- Retain a cyber security expert to assess the breach.
- Report to your insurance company.

FTC SAFEGUARDS RULE

FTC SAFEGUARDS RULE

- The purpose of the rule is to ensure that entities covered by the Rule maintain safeguards to protect the security of customer information.
- This rule was amended in 2021 to consider current technology.
- The Safeguards Rule requires covered financial institutions (including tax preparation firms) to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.
- The Rule defines customer information to mean “any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.” (The definition of “nonpublic personal information” in Section 314.2(l) further explains what is – and isn’t – included.)
- The Rule covers information about your own customers and information about customers of other financial institutions that have provided that data to you.

IRS PUBLICATION 5708

CREATING A WRITTEN INFORMATION SECURITY PLAN FOR YOUR TAX AND ACCOUNTING PRACTICE

Vandenack Weaver LLC
402.504.1300
VWTlawyers.com

INTRODUCTION

- IRS Publication 5708 discusses the requirements for tax preparing firms to create a Written Information Security Plan, a “WISP.”
- The Gramm-Leach-Bliley Act (GLBA) is a U.S. law that requires financial institutions to protect customer data.
- In its implementation of the GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule to outline measures that are required to be in place to keep customer data safe. One requirement of the Safeguards Rule is implementing a WISP.
- Under the GLBA**, tax and accounting professionals are considered financial institutions, regardless of size**. Financial institutions subject to the Safeguards Rule include mortgage brokers, real estate appraisers, universities, nonbank lenders, and check cashing businesses.

WRITTEN INFORMATION SECURITY PLAN REQUIREMENTS

- As a part of the plan, the FTC requires each firm to:
  - Designate one or more employees to coordinate its information security program.
  - Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks.
  - Design and implement a safeguards program, and regularly monitor and test it.
  - Select service providers that can maintain appropriate safeguards by ensuring your contract requires them to maintain safeguards and oversee their handling of customer information.
  - Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

WHAT IS APPROPRIATE TO BE INCLUDED

- The publication discusses that a security plan should be appropriate to the firm's size, scope of activities, complexity, and the sensitivity of the customer data it handles. There is no one-size-fits-all WISP. For example, a solo practitioner can use a more abbreviated and simplified plan than a 10-partner accounting firm (note that the publication's language directly referenced accounting firms).
- Three areas are discussed for focus in a WISP:
  - Employee management and training. This should be consistent and continuous.
  - Information systems.
  - Detecting and managing system failures.
- It is noted that the WISP is meant to be an "evergreen" document, regularly reviewed and updated due to changes in technology and to the size, scope, and complexity of the firm's business. Remember to train employees whenever changes are made.
- Do you consider the changes in the nature of your practice and how it may affect the data security needed. For example, if the nature of the confidential data you hold changes due to increased scope of your services, it may cause you to be in a higher "tier" of required data security to protect that data.

ADDRESSING THE WISP WITH EMPLOYEES

- The IRS references creating an Employee/Contractor Acknowledgment of Understanding document for all personnel to keep a record of training and understanding of the policies in your WISP.
- The publication references “contractors.” Consider whether this means any third-party contractors that are provided access to the firm’s technology infrastructure must be included in training and implementing a WISP.
- Create a documentation trail of training.
  - Documentation should reflect compliance and accountability.
  - The publication recommends that these acknowledgments be updated at annual training intervals and kept on file. Best practices should be more often.
- The WISP should be maintained in a format that others can easily read, such as PDF or Word. Making a WISP available to employees for training purposes is encouraged.
- Designate your WISP coordinator to send out weekly security tips. Send in a manner that requires a response.

WISP AND THIRD-PARTY VENDORS

- Third-party vendor is any person or organization who provides a product or service to your organization.
- Examples: Janitorial services; Data centers; SaaS providers.
- The sample WISP provided in the publication includes the following statements regarding third-party vendors:
  - "…Requiring third-party service providers to implement and maintain appropriate security measures that comply with this WISP…"
  - "…Any third-party service provider that does require access to information must be compliant with the standards contained in this WISP at a minimum..."
- Manage point of contact with third-party vendors.

WISP AND THIRD-PARTY VENDORS (cont)

- Exceptions listed are tax software vendors and e-Filing transmitters, state and federal tax authorities. IRS Publication 1345 is referenced for more information.
- To vet third-party vendors, use an interview process. Hire an expert to assist with vetting. This process is not explained in the publication but there are industry compliance resources that provide information on vetting.
- Conduct an audit that evaluates the vendor's security compliance. Set up monitoring that tracks any changes in the vendor's risk profiles.
- Research and collect information on safety statistics, certificates of insurance and audit reports that illustrate vendor competency.
- Request certificate of insurance.
- Consider whether the vendor is critical to your operation.
- Focus on your highest risks first. Example: Vendor who houses sensitive data on their systems.

SAMPLE OUTLINE FOR A WISP-1

- A sample outline is provided in the publication.
- Define the WISP objectives, purpose, and scope.
- Identify responsible individuals.
  - List individuals who will coordinate the security programs as well as responsible persons.
  - List authorized users at your firm, their data access levels, and responsibilities.
- Assess Risks.
  - Identify Risks.
  - List types of information your office handles.
  - List potential areas for data loss (internal and external).
  - Outline procedures to monitor and test risks.
- Inventory Hardware.
  - List description and physical location of each item.
  - Record types of information stored or processed by each item.

SAMPLE OUTLINE FOR A WISP - 2

- Document Safety Measures in place
  - Suggested policies to include in your WISP:
    - Data collection and retention
    - Data disclosure
    - Network protection
    - User access
    - Electronic data exchange
    - Wi-Fi access
    - Remote access
    - Connected devices
    - Reportable Incidents
  - Draft Employee Code of Conduct
- Draft an implementation clause
- Attachments

SAMPLE TEMPLATE FOR A WISP

- The publication includes a 12-page template of language to incorporate into a WISP. It also includes numerous sample attachments, including rules of behavior for protected information, security breach procedures, an employee acknowledgement of understanding, and more.
- A PDF of the publication and sample documents can be accessed at https://www.irs.gov/pub/irs-pdf/p5708.pdf

CLIENT COMMUNICATIONS AND SECURITY

TECH DEVICES CREATE RISKS

- ABA Ethics Opinion 477 updates Ethics Opinion 99-413 to reflect the now common use of tech such as tablet devices, smartphones, and cloud storage. While this applies to lawyers, it provides good information for any tax professional.
- Each device and each storage location offers an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation.
- Consider all tech devices and access to data in designing a security plan.
- ABA has published a Cybersecurity Handbook that is useful for any tax professional.

CONFIDENTIALITY AND COMMUNICATION

THE DUTY OF CONFIDENTIALITY

- ABA Model Rule of Professional Conduct 1.6 provides that a lawyer shall maintain confidentiality of information. “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of … information relating to representation of a client.” Similar rules apply to accountants and other financial professionals.
- Comment 18 to Rule 1.6 requires acting reasonably with respect to safeguarding client information.
- Factors to be considered in determining the reasonableness of the efforts include:
  - sensitivity of the information
  - likelihood of disclosure if additional safeguards are not employed
  - the cost of employing additional safeguards
  - the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients
- A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule.

FORMS OF CLIENT COMMUNICATIONS?

- Email
- Text
- Voice
- Instant Messaging
- Shared Calendars and Task Lists
- White Boards
- Collaboration Platforms
- Videoconferencing Services
- Social Media
- Consider all forms of communication in designing a security plan.

DISPARITIES AMONG FIRMS

- A recent ILTA survey notes that there is a disparity in this area as between large firms (which are all over security issues and typically required to be by clients who demand proof of security, and midsize firms who are aware of the issues, and small firms who may be aware of the issues but are not proactively addressing the issue.)

- A small or mid-size firm may want to engage an outside consultant to review communications processes and provide recommendations and implementation strategies for ensuring security of communications. BUT don't be the small firm that makes the news!

- A small firm could use technology as a differentiator.

FIRMS MUST TRAIN AND SUPERVISE

- ABA Model Rule 5.1 directs attorneys who have supervisory authority over other attorneys to make reasonable efforts to ensure the supervised attorneys conform with the Rules of Professional Conduct. Similar rules apply to other professionals.
- ABA Model Rule 5.3 requires attorneys with supervisory authority over non-attorneys inside and outside the firm to make reasonable efforts to ensure the non-lawyer's conduct comports with an attorney's professional obligations.
- Don’t be the firm whose paraprofessional let her kids play on the home computer resulting in some client emails being posted on Instagram.

CONFIDENTIALITY AND COMMUNICATION

SEE ABA FORMAL OP. 477R AS AN EXAMPLE

- Client matters involving proprietary information in highly sensitive industries, such as health care, banking, and defense may present a higher risk of data theft.
- Professionals should understand how their firm's electronic communications are created, where the client data resides, and what avenues exist to access that information.
- Professionals must protect against unauthorized disclosure in client communications by using appropriate electronic security measures including, for example, by: secure internet access methods to communicate, access, and store client information; unique complex passwords, changed periodically; firewalls and anti-malware, anti-spyware, and anti-virus software on all devices containing client confidential information; and all necessary security patches and updates to operational and communications software.

MORE FROM ABA Formal Op. 477R

- Different communications require different levels of protection. At the beginning of the attorney-client relationship, the attorney and client should discuss, and in cases involving sensitive communications agree, on appropriate levels of security for each electronic communication.
- Professionals should mark applicable communications as "privileged and confidential".
- Professionals must establish policies and procedures and periodically train employees, subordinates, and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients.

AI AND CONFIDENTIALITY

- “The use of some AI tools may require client confidences to be “shared” with third-party vendors. As a result, professionals must take appropriate steps to ensure that their clients’ information appropriately is safeguarded. Appropriate communication with the client also is necessary.”
- “To minimize the risks of using AI, a professional should discuss with third-party AI providers the confidentiality safeguards in place. A professional should inquire about “what type of information is going to be provided, how the information will be stored, what security measures are in place with respect to the storage of the information, and who is going to have access to the information.” AI should not be used in the representation unless the professional is confident that the client’s confidential information will be secure.”

RESOURCES

BOOKMARK/CONNECT TO RESOURCES

- Publication 4557 https://www.irs.gov/pub/irs-pdf/p4557.pdf
- Authorized IRS e-file Providers of Individual Income Tax Returns https://www.irs.gov/pub/irs-pdf/p1345.pdf
- Small Business Information Security: The Fundamentals https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- Stakeholder Liaison Contacts https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts

BOOKMARK/CONNECT TO RESOURCES (cont.)

- Subscribe to IRS Quick Alerts: https://www.irs.gov/e-file-providers/subscribe-to-quick-alerts
- Follow IRS on social media. https://www.irs.gov/newsroom/irs-social-media
- FTC Safeguards Rule. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
- IRS Publication 5708. https://www.irs.gov/pub/irs-pdf/p5708.pdf

THANK YOU!

- Contact Information:
  - mvandenack@vwtlawyers.com
  - https://www.linkedin.com/in/mary-vandenack-508020a/
  - Twitter: mvandenack
  - Instagram: mvandenack