Texas Society of Certified Public Accountants
CPE Foundation, Inc.

61st Annual TSCPA Tax Institute

In World Where Privacy is a Moving Target, Tax Professionals Need to Consider Social Media, Disclosures, Conflicts of Interest and Cloud Computing in Their Practice

William C. Nantz, CPA, CFF, CGMA, PTIN, MBA, JD

November 20-21, 2014
San Antonio and Richardson (Dallas)

Presentation: Tax Professionals have a duty to protect their client's personal identifying information. The moving target of privacy requirements may be confusing and this presentation will address major issues surrounding Social Media, Disclosures, Conflicts of Interest and Cloud Computing.

William C. Nantz, CPA, CFF, CGMA, PTIN, MBA, JD, "Bill", provides is a Forensic Accounting Professor at HCC and provides forensic accounting services through William C. Nantz, CPA, a firm licensed as an accounting firm by the TSBPA. This presentation and the related article are provided as general information only and should not be construed as legal advice. This presentation and article are not intended to be applied to any particular situation as such application requires knowledge and analysis of the specific facts involved. Bill is also the founder of the Nantz Law Firm (the Nantz Law Firm is not a CPA firm) and Bill may be contacted at 713.542.5477 or bill@nantzlaw.com.

In World Where Privacy is a Moving Target, Tax Professionals Need to Consider Social Media, Disclosures, Conflicts of Interest and Cloud Computing in Their Practice

Presented by:

William C. Nantz, CPA, CFF, CGMA, PTIN, MBA, JD

Table of Contents

William C. Nantz, CPA, CFF, CGMA, PTIN, MBA, JD, "Bill", provides is a Forensic Accounting Professor at HCC and provides forensic accounting services through William C. Nantz, CPA, a firm licensed as an accounting firm by the TSBPA. This presentation and the related article are provided as general information only and should not be construed as legal advice. This presentation and article are not intended to be applied to any particular situation as such application requires knowledge and analysis of the specific facts involved. Bill is also the founder of the Nantz Law Firm (the Nantz Law Firm is not a CPA firm) and Bill may be contacted at 713.542.5477 or bill@nantzlaw.com.

A copy of this presentation, many of the materials discussed herein, and other presentations presented by Bill are located at his HCC website: http://learning.hccs.edu/faculty/william.nantz. Please feel free to review these materials.

In World Where Privacy is a Moving Target, Tax Professionals Need to Consider Social Media, Disclosures, Conflicts of Interest and Cloud Computing in Their Practice

Presented by:

William C. Nantz, CPA, CFF, CGMA, PTIN, MBA, JD

Privacy concerns are raised when CPA firms and its employees use social media and social networking sites. Protection of a client's sensitive personal identifying information in the online environment requires new strategies to properly protect the client's privacy. The online environment creates new complications regarding the use and protection of a client's sensitive personal information. The State of Texas and the federal government have implemented rules and regulations regarding the retention and use of personal identifying information. The AICPA weighed in on privacy matters by creating Generally Accepted Privacy Principals or GAPP. The GAPP checklist is found here:

> http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/PrivacyServices/DownloadableDocuments/CPA_Firms_Privacy_Checklist.pdf.

The AICPA outlines the best business practices of CPAs including adoption of a Privacy Policy. This is not the law, but is the best business practice for a CPA because a policy informs clients that the CPA protects his or her client's sensitive personal identifying information.

CPAs are required to properly safeguard and properly dispose of personal identifying information, yet are typically exempt from the requirement to adopt a Privacy Policy and exempt from the requirement to send annual privacy notices to clients. Regulations are tightening regarding the safeguarding of personal identifying information, regardless of how the information was obtained. Following the AICPA GAPP checklist is not required by law and given the rapid changes in social media and the move to cloud, CPAs need to carefully analyze the online environment in which they operate and adopt the appropriate policies and procedures.

Privacy in the Online Environment

The online environment creates business opportunities while posing challenges for CPAs. Many CPAs use social media and social network sites to maintain both business and personal relationships. CPAs also allow the business and personal information used on these sites to cross over. The crossing over of personal and business on both social media and social network sites creates unforeseen issues for CPAs. As well, management of the technology supporting social media and social network sites is rapidly changing and the rules regarding the use of the technology in the workplace is not keeping up with the technology. These challenges put the management of a CPA's practice to the test.

The Texas State Board of Public Accountancy recently fined a CPA for improperly using his CPA designation on Facebook. As best as I can discern, this Texas CPA did not license his firm, a separate licensing requirement in Texas. His unlicensed firm provided financial planning services and on Facebook he wrote his name, Tim Smith, CPA while listing himself as the owner of Smith Investment Advisors (not real names). Since he did not say that Smith Investment Advisors was not a CPA firm on his Facebook profile, he was fined a small amount. This is just one example of the online environment in which CPAs operate.

There is a general notion that there is no privacy in the online environment, and I think this is correct. It may be better stated that the Internet not discern between one's private life and one's public life. Facebook, Twitter, Instagram, Linkedin, and any other site where personal or business information is shared, are places where there is no privacy. The notion that there is privacy on these sites is just a misconception and one's business reputation is the same as one's online reputation.

The problem is that most people mix business and personal information on the Internet. If Facebook is just for friends, the notion that telling your friends that you own a business and you are a CPA is probably not a rule violation. Also, it is incredibly hard to prosecute such a communication. But telling your online friends that you are a CPA is a form of publishing the information and there are rules to be followed. The issue is that people use Facebook, and other such sites, to mingle with their friends, co-workers, customers and business prospects but forget that the information posted on social media sites is published in a public forum.

How do you go about controlling your firm's reputation when your employees post your firm as their employer on social media sites? Many employers want their employees to post such information on social media sites because it is perceived as marketing. Posting raises issues because friends, co-workers, customers and business prospects are mingling in an online conversation that may not be able to be erased because it is recorded on the Internet.

Bad things can happen when Internet friends turn ugly. An example is when an employee links his or her Facebook page to someone that he or she does not know that well. Now this unknown person links his or her profile to the employee's friends, co-workers, customers and business prospects' profiles on Facebook. The employee, probably while intoxicated, video conferences via Skype[1] with the unknown person while entering a state of au naturel and poses in various delicate situations. The unknown person records the video conversation and then blackmails the employee with the recording. The unknown person now has a direct link with the employee's friends, co-workers, customers and business prospects with which to attempt to expose the employee. This has happened.

[1] Skype is basically an Internet application that provides video conferencing and either party may record the video chat. Skype provides may other services and may be accessed from a smartphone, tablet, phablet, or computer via the Internet.

Loss of reputation may be the highest cost of an employee's troublesome posts on the Internet. Another example of what may happen to an employee, and possibly the reputation of your firm, is found in Pax Dickinson's story. He was the Chief Technology Officer (CTO) of Business Insider and claims on his blog he was Internet shamed and then fired because he made off-color jokes on Twitter.[2] Pax says, "When Valleywag posted their story about me, they dug through years of tweets to find the ones most damaging to take out of context, mostly tweets that had been posted years before to an audience of two dozen friends."[3] He goes on to state:

> No one at Valleywag ever attempted to contact me, before the article went up or afterwards. In the following days, I was declared by literally every media organization that I have ever heard of, and many that I haven't, to literally be The Devil. CNN hilariously posted a picture of me in a Halloween costume wearing horns. Other outlets used a different Halloween pic of me as a brogrammer with a popped collar. (Don't tweet pics of your Halloween costumes kids. It'll come back to bite you. Trust me.)[4]

The moral of this story is that you and your employee's "personal" posts on social media sites are not private and that the "private" postings of your employee's are now representative of your firm or company. Any posts made by employees on the Internet speak directly to your company or firm's values and ethics. A well developed reputation may be lost by an employee's troublesome postings on a social media site.

Facebook, Twitter, Instagram, Linkedin and any other social media site may be accessed by a smartphone user via wifi or an app on the phone. Cell phones are not longer phones; cell phones are truly smartphones that take the place of a computer. Smartphones allow one to read and answer emails, take photographs, record video, prepared documents and spreadsheets, read attachments to emails and perform any other computer function. Smartphones are essentially pocket sized computers. Verizon describes the smartphone experience as one where you can do "everything from surfing the web to watching movies to social media and gaming."

The smartphone experience is enhanced by use of moblie apps designed to run on smartphones; mobile apps are computer programs loaded on the phone. This means that your employees have apps that allow them to experience everything from the "privacy" of their phone including gambling, watching porn, surfing the net, Facebooking[5], cruising Tender[6], or who-knows-what-else while sitting in their office or cubicle and firing up their new smartphone apps.

---

[2]Moral Panics and the Death of Fun. http://paxdickinson.wordpress.com/2014/10/22/moral-panics-and-the-death-of-fun/ (Nov. 3, 2014).

[3] Id. Here is a list of the tweets: http://unvis.it/valleywag.gawker.com/business-insider-ctos-is-your-new-tech-bro-nightmare-1280336916

[4] Id.

[5] Facebooking is a verb used to describe the activity of logging into Facebook in order to create a profile, share personal information, or meet other members. http://www.netlingo.com/word/facebooking.php (Nov. 3, 2014).

[6] Tinder is the latest in a slew of location based hook-up partner finding apps that use GPS to locate future sex-mates: http://www.theatlantic.com/national/archive/2013/02/tinder-hook-app-women-actually-use/317875/ (Nov. 3, 2014).

Apps are not private and can share much, if not all of, the information saved on a smartphone. According to Wired, one of the Flashlight apps "is designed do location tracking, read my calendar, use my camera, gain access to unique numbers that identify my phone, and then share data…"[7] According to Snoopwall "Some of the Flashlight Apps write settings and have access to your device storage; maybe to install additional backdoors or remote access Trojans (RATs)."[8] Watch the video here[9] discussing Flashlight Apps and the transfer of private information. Flashlight Apps are not the only apps that may have access to your private information.

Many apps download all types of information off your smartphone. A recent article shared that in "a separate study by cloud security firm Zscalar into privacy issue with iOS apps found that 96 per cent of iOS apps require email, address book (92 per cent), location (84 per cent), camera (52 per cent), calendar (32 per cent) permissions."[10] An app's privacy policy typically outlines the information it is downloading, but it may not tell you where the information is ultimately shared. This is a new area that needs to be addressed by employers when employees use their smartphone as a portable work station.

Social Media Policy

CPAs and their firms need a Social Media Policy to direct employees and the firm's behavior on the Internet. The examples outlined above demonstrate that a firm and its employees need to monitor what is posted on any social media site and on the Internet in general. It is important to monitor a firm's online reputation and provide social media training to employees.

Many firms are now performing a pre-employment review of each employment candidate's Facebook account. Given the experiences of some employers, this review should be performed on all social media in which the candidate participates. One of my students was ask to look at a job candidate's Facebook page and noticed a fair number of references to cannabis. The candidate was not hired. Many job candidates will feel this type of review is intrusive.

The candidates are not considering the reputation of the potential employer. The cross-over of business and personal affairs through the use of social media is one area in which the rules and related laws have not caught up to the online environment. The Internet reputation of an employee is the reputation of the firm. Regulating Internet behavior is an issue because there is no guidance and no regulations regarding an employer's management of an employee's behavior on the Internet and use of social media.

The use of social media allows CPAs to market their firm and services to a large number of people and organizations, but also creates a number of pitfalls that need to be monitored. CPAs

[7] *The Hidden Privacy Threat of … Flashlight Apps?* http://www.wired.com/2014/10/iphone-apps/ (Nov. 3, 2014).
[8] *Snoopwall Flishlight Apps Threat Assessment Report.* http://www.snoopwall.com/wp-content/uploads/2014/10/Flashlight-Spyware-Appendix-2014.pdf
[9] http://benswann.com/exclusive-top-10-flashlight-apps-are-stealing-your-data-even-pics-off-your-phone/
[10] *The TRUTH about LEAKY, STALKING, SPYING smartphone application. http://www.theregister.co.uk/2014/01/31/smartphone_app_spy_risks/ (Nov. 3, 2014).*

should track changes in social media sites because the sites are constantly upgrading and changing. Also, the CPA and the firm should review what is being said on the internet about the individual or the firm. There are several tools that allow you to track your online reputation. Some of these tools:

> Trackur A social media monitoring tool that offers instant notifications when your brand is mentioned.
>
> Naymz A useful tool for tracking your social influence, which is closely tied to your online reputation.
>
> Brandseye Get email notifications when your brand is mentioned online, and track conversations and compares metrics with your internal data.
>
> Rankur You can narrow your results by demographics and other data to really tune in to how your marketing messages and branding efforts are resonating with a particular subset of your audience.
>
> SocialMention A totally free tool, SocialMention is a search engine that scours the social sphere for mentions of your brand, or a competitor, or any key phrase you type in.
>
> Google Alerts Set up alerts for any search terms you want, such as your company name or targeted phrases relevant to your niche, then specify the types of results you want and how often.

These tools allow you to track your online reputation across the Internet.[11] Reputation tracking is important, but it may not cover employee's personal posts to many social media sites, especially posts that do not specifically involve your firm's name.

A social media policy needs to specifically consider Linkedin because most employees have a profile that is linked to your company or firm. Also, Linkedin is an inexpensive method to market your firm with possible associations between you, your firm and other people or entities. One of the pitfalls of Linkedin is that you consent to using your image in Linkedin advertising:

> LinkedIn assumes that you consent to LinkedIn's use of your image in the advertising of its sponsor's products. If you recommend your CPA firm, and your CPA firm purchases advertising on LinkedIn, your photo may appear in that advertising.[12]

This means that your image or brand may be linked to other parties without your consent. This is just one of the pitfalls of Linkedin. A careful review of Linkedin and all other social media on a regular basis needs to be done to ensure that your message and brand are properly represented.

With the growth of social media, a Social Media Policy needs to be implemented. This policy needs to provide the guidelines outlining your firm's or company's expectations. Each Social Media Policy needs to be tailored to fit the businesses' expectations. The policy should address how the company is to be represented on the Internet and what behavior is expected from each employee. Each employee should review, agree to its terms, and sign a copy of the policy.

---

[11] *6 Tools Than Make Tracking Your Online Reputations Easy.* https://www.americanexpress.com/us/small-business/openforum/articles/online-reputation-management-tools/ (Nov. 3, 2014).

[12] *LinkedIn Assumes You "Opt-in" to Social Media Advertising.* http://dataprivacy.foxrothschild.com/2011/08/articles/employee-social-media-use-1/psa-linkedin-assumes-you-optin-to-social-media-advertising/ (Nov. 3, 2013).

Privacy Policy

As a CPA, you may find yourself collecting an individual's personal identifying information in many different circumstances. Basically, you are required to keep certain information private and to protect this information from misuse. With advances in the ability to utilize Cloud Computing through numerous computing devices such as a desktop, laptop, tablet, net book and even a smart phone; it is a challenge for a CPA to ensure that the private information remains private.

Protection of sensitive personal identifying information of clients and employees is of the utmost importance because of recently enacted federal and state laws. The State of Texas and the federal government have implemented rules and regulations regarding the retention and use of personal identifying information. Regulations are tightening regarding the safeguarding of personal identifying information, regardless of how the information is obtained. Most CPAs are exempt from the rules requiring the adoption of a Privacy Policy and the requirement to send annual privacy notices to clients, but there are no exemptions regarding the requirement to properly safeguard and properly dispose of clients' personal identifying information.

Collection of sensitive personal identifying information may go beyond the information collected from clients and may include information collected regarding employees, potential employees, information collected about a client's employees or customers, and any other situation where sensitive personal identifying information is collected. If the CPA collects the client's social security information for purposes outside of an agreement to provide professional accounting services, such as for insurance sales or stockbroker purposes, the exemption does not apply and the CPA should adopt a privacy code and make the privacy policy available to the client. Also, if a license holder fails to renew his license, the Accountant-Client privilege will no longer be applicable and the unlicensed CPA would be required to adopt a privacy code and make the privacy policy available to the client.

Protection and proper disposal of a client's sensitive personal identifying information is now the law. The Federal Trade Commission requires the protection of taxpayer information and proper disposal of taxpayer information in a manner that protects the unauthorized access to or use of the information under the Safeguard Rule promulgated by the Gramm-Leach-Bliley Act. The IRS outlines this obligation in its *Safeguarding Taxpayer Information, Quick Reference Guide for Business* found at http://www.irs.gov/pub/irs-pdf/p4600.pdf. CPAs are not exemption from the state and federal requirements to safeguard and properly dispose of the sensitive personal identifying information they collect.

Texas takes this a step further and specifically requires the shredding, erasing or modification an individual's personal information, not just the taxpayer information. Disposal of confidential information needs to follow Business & Commerce Code Section 35.48 *Retention and Disposal of Business Records to an Outside Party*, and needs to include the appropriate disposal of the hard drives of individual computers. Upon destruction, the personal information must be made unreadable or indecipherable. Texas law defines sensitive personal identifying information as an

individual's first name or initial and last name used in combination with one or more of the following personal identifying information:

a. date of birth;
b. social security number or other government-issued identification number;
c. mother's maiden name;
d. unique biometric data, including the individual's fingerprint, voice data, or retina or iris image;
e. unique electronic identification number, address, or routing code;
f. telecommunication access device as defined by Section 32.51, Penal Code, including debit or credit card information; or
g. financial institution account number or any other financial information.

Both the Federal Trade Commission and the Texas law permit the disposal of sensitive personal identifying information to be made by a document destruction service that the CPA has identified and performed due diligence regarding the service's compliance with proper eradication and erasure of the sensitive personal identifying information. A CPA may contract with an individual or other entity engaged in the business of disposing of records, which will dispose of Client personal information by either shredding or obliteration. When computers are destroyed, the hard drives need to be removed and destroyed separately.

The Texas Legislature amended the Business and Commerce code to exempt individual and firm CPA license holders and their partners, members, officers, shareholders, or employees from the requirement to adopt a privacy policy for clients who qualify for the Accountant-Client privilege outlined in the Texas Public Accountancy Act Section 901.457. The trigger permitting avoidance of the privacy policy requirements is a client's qualification for the Accountant-Client privilege. As well, the Accountant-Client privilege may require the CPA to not disclose a client's information or records. Requests for access to these records may come from many sources.

General Disclosure Rules

A CPA may be obligated to respond to requests for personal information of their clients, the CPA's work papers and other documents or private information under the CPA's custody or control. Generally, personal information may only be disclosed as directed by a client or as otherwise permitted or required by court order, appropriate taxing authority, SEC or grand jury subpoena, legal process, law, or regulation. Further, a Client's personal information may be disclosed for the purposes of professional peer-review or Public Company Accounting Oversight Board inspection. If the request is for audit work papers, be careful because audit "documentation is the property of the auditor, [and] … the auditor should adopt reasonable procedures to maintain the confidentiality of that information."[13]

[13] AU Section 339, *Audit Documentation*, .31 – .33. P. 2035.

A request may come from "current and former clients, lawyers, civil and criminal investigators, lenders, and others. …When responding to records requests, CPA firms must consider all applicable professional standards, regulations, and statutes pertaining to client confidentiality, privacy, and requests to produce records. These include, but are not limited to, the following:

- AICPA Code of Professional Conduct (the AICPA Code);
- State board of accountancy regulations;
- Regulations issued by the SEC, PCAOB, and state securities regulators;
- Regulations and laws applicable to the client's industry;
- State privacy laws;
- Circular 230, *Regulations Governing Practice Before the Internal Revenue Service* (31 C.F.R. Part 10);
- Internal Revenue Code (IRC) Secs. 6103(c) and 7216; and
- Federal privacy laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act."[14]

The best business practice is to require that the request for any type of personal information be made in writing and that all responses be written. Regardless of the reason why the CPA collected or retained the personal information, the CPA must maintain personal information in a confidential manner and use commercially reasonable safeguards to prevent unauthorized access to personal information while appropriately responding to requests for the protected documents. The CPA should also protect any privileges attached to the information it is protecting.

Accountant-Client Privilege in Texas and under U.S. Code Sec. 7525

Contrary to popular belief, there is an Accountant–Client privilege under both Texas law and federal tax law. The Accountant-Client privilege in Texas is based upon an agreement to provide professional accounting services between a CPA and his or her client for any type of accounting services.[15] Under this privilege

> "A license holder or a partner, member, officer, shareholder, or employee of a license holder may not voluntarily disclose information communicated to the license holder or a partner, member, shareholder, or employee of the license holder by a client in connection with services provided to the client by the license holder or a partner, member, shareholder, or employee of the license holder, except with the permission of the client or the client's representative.[16]

The same Texas Accountant-Client privilege is also found in the Texas Administrative Code under Rule §501.75, Confidential Client Communications, wherein it similarly states that a CPA "shall not voluntarily disclose information communicated to him by the client relating to, and in

[14] *When parties come knocking for client records.* http://www.journalofaccountancy.com/Issues/2013/Feb/20126773.htm.
[15] Texas Public Accountancy Act Section 901.457.
[16] Sec. 901.457, Accountant-Client Privilege, found in http://www.tsbpa.state.tx.us/pdffiles/TSBPAACT.pdf.

connection with, professional accounting services or professional accounting work rendered to the client by the person. Such information shall be deemed confidential."[17] This privilege applies to all accounting work, not just tax work. It also applies to accounting employees holding a CPA license, not just CPAs providing tax services.

The federal tax law Accountant–Client privilege is found in U.S. 26 Code Sec. 7525.[18] This federal tax Accountant – Client privilege "is based upon the common law protections of attorney-client privilege to a client who is communicating with a federally authorized tax practitioner regarding tax advice. The practitioner must be authorized under federal law to practice before the IRS, and such practice must be subject to federal regulation under 31 U.S.C. Section 330. Authorized tax practitioners include licensed attorneys, CPAs, enrolled agents, and enrolled actuaries."[19] A tax return preparer who solely prepares a return does not provide a client with the Accountant–Client privilege because the tax return preparer is not providing tax advice.

A pitfall under the Texas rule is that attorneys may issue subpoenas without a court's approval and this is a legitimate type of subpoena. But a subpoena issued by a lawyer, even a District Attorney or employees of the District Attorney, does not permit a CPA to waive the Accountant-Client privilege. Section 901.457(3) says that the request must be a court order signed by a judge, addressed to the license holder, mentions the client by name, and requests specific information regarding the client. A subpoena issued by a lawyer is not a court order signed by the judge. If you receive a subpoena that is not signed by the judge, properly and promptly object to the subpoena in the court from where it was issued. Also, promptly and inform your client of the receipt of any subpoena or request for documents.

The claim of privilege may be overridden by exceptions, but don't release any of your client's information without consulting the law. If necessary, assert any privilege and withhold any documents until the matter is cleared by the court or by written agreement of the parties, including the signed approval of your client. The privilege may be waived by the client or the taxpayer, but a CPA does not want to inadvertently waive the privilege. Prior to releasing any documents, also review U.S. Code Section 7216, discussed below, to ensure that you are not waiving your client's privilege. U.S. Code Section 7216 applies to tax returner prepares as well as authorized tax practitioners.

---

[17] Texas Administrative Code, Title 22, Part 22, Chapter 501, Subchapter C, Rule Sec. 501.75, *found at* http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=22&pt=22&ch=501&rl=75

[18] 26 U.S. Code § 7525 - Confidentiality privileges relating to taxpayer communications, found at http://www.law.cornell.edu/uscode/text/26/7525 .

[19] *Protecting Communications and Documents From IRS Summons Enforcement.* http://www.aicpa.org/publications/taxadviser/2013/april/pages/burilovich_apr2013.aspx?action=print#fnref_4

Tax Preparer Disclosures under Sec. 7216

"Internal Revenue Code §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 or imprisoned not more than one year or both, for each violation."[20] The civil side of this matter in found in Internal Revenue Code §6713 imposing a "penalty of $250 on any person who is engaged in the business of preparing, or providing services in connection with the preparation of returns of tax, or any person who for compensation prepares a return for another person, and who discloses any information furnished to him for, or in connection with, the preparation of any such return or uses any such information for any purpose other than to prepare, or assist in preparing, any such return"[21]The civil penalty is imposed for any disclosure while the criminal penalty requires a knowing or reckless disclosure. These penalties may be levied against return preparers or authorized tax practitioners.

A taxpayer must knowingly and voluntarily consent to disclose tax return information. The disclosure may be made using an electronic signature or pen-and-ink. The signatures need to be dated and include "the names of the tax return preparer and the taxpayer and that specify the nature of the disclosure(s), to whom the disclosures will be made, and details on the data to be disclosed."[22] CPAs who are engaged in tax return preparation and tax planning services need to become familiar with Treas. Reg. section 301.7216 and Revenue Procedure 2008-35, the authoritative guidance with respect to a preparer's disclosure or use of tax return information.[23] Yet, this is not the only penalty for the improper disclosure or use of tax return information.

"IRS Circular 230, Section 10.51(a)(15), indicates a practitioner may be sanctioned for disreputable conduct for willfully disclosing or using a tax return or tax return information in a manner not authorized by the Code."[24] Sanctions related to IRS Circular 230 are typically censure, suspension, or disbarment. This means that the tax practitioner, and possibly a tax preparer, will lose his ability to perform tax work. A discussion of the procedure is found at http://www.irs.gov/Tax-Professionals/Enrolled-Agents/Circular-230-Disciplinary-Proceedings. Issues surrounding tax preparers and the applicability if Cir. 230 to tax preparers has not been resolved at the time of the preparation of this presentation.

Outsourcing:

Another issue facing tax return preparers is outsourcing. "Disclosing tax return information to another tax return preparer that is assisting in the preparation of the return or providing auxiliary services in connection with preparing the return generally does not require the consent of the taxpayer. However, if the other tax return preparer is located outside the United States or any territory or possession of the United States, the taxpayer must agree and sign a form consenting

[20] http://www.irs.gov/uac/Section-7216-Frequently-Asked-Questions
[21] *Id*.
[22] *Id*. Refer to Treas. Reg. §301.7216-3(a)(3) and Revenue Procedures 2013-14 and 2013-19 for more specific information regarding consent forms and certain language and warnings that the consent forms must contain.
[23] Treas. Reg. section 301.7216 was released in January 2008, and is found at: http://www.irs.gov/irb/2008-05_IRB/ar07.html; and as stated above, is effective on January 1, 2009. Rev. Proc. 2008-35 is found at: http://www.irs.gov/irb/2008-29_IRB/ar13.html.
[24] Current Tax Return Disclosure Issues Involving Sec. 7216.
http://www.aicpa.org/publications/taxadviser/2013/august/pages/tpr_bond_aug2013.aspx

to the disclosure."[25] Revenue Procedure 2013-14, section 5.04(e) outlines specific language that must be included in the consent form.[26]

"If social security numbers are included in documents for which the tax return preparer has obtained the consent of the taxpayer to disclose the tax return preparer must redact or mask any social security number before disclosing the tax return information to a return preparer outside the United States. There is an exception. Social security numbers may be disclosed to tax return preparers located outside the United States if taxpayer consent is obtained and both the sending and receiving tax return preparers maintain adequate data protection safeguards defined in Revenue Procedure 2013-14, section 5.07."[27] This section also requires the warning that "If you do consent to the disclosure of your tax information, federal agencies may not be able to enforce United States laws that protect the privacy of your tax return information against a tax return preparer located outside of the United States to whom information is disclosed."

Comfort Letters:

One of the issues facing tax professionals is the request for a Comfort Letter. The request is typically made from a lender of the taxpayer. The request is typically for more than just the release of the tax return. Great care needs to be taken when sending a tax return to a taxpayer's lender. My personal advice is to send a copy of the tax return to the taxpayer and ignore the request for the lender. *Allow the taxpayer to send a copy of the tax return to the lender*.

The problem with the comfort letter is that "[s]ome of these requests require the use of specific language in the responding letter, including use of the words "certify" and "verify." These words are not associated with and are unrelated to the scope of a typical engagement for tax return preparation and would normally be used only as part of an attest engagement."[28] This means that you are, at a minimum, being asked to prepare some type of audit report or perform some type of agreed upon procedures on the financial information provided in the tax return. The lenders "are attempting to shift the responsibility for anything that could go wrong in the future with the loan to the tax return preparer for misrepresenting the client's financial position. There is a communication gap between the requesters of this information and CPAs as tax preparers; no resolution appears to be on the horizon."[29] If you send the tax information to the entity requesting the comfort letter, make sure you receive the appropriate release from you client. The better business practice is to forward the request to the taxpayer and to not respond to the party requesting the comfort letter.

Preparer Penalties and disclosure requirements:

The CPA Journal provides an extensive review of tax return penalties.[30] One of the penalties is related to the obligation of a tax return preparer to either retain copies for themselves or maintain a list of all returns and claims prepared which includes clients' names and Social Security numbers. The copies or list must be kept for three years after the close of a return period and

[25] Q. 14. http://www.irs.gov/uac/Section-7216-Frequently-Asked-Questions.
[26] http://www.irs.gov/pub/irs-drop/rp-13-14.pdf
[27] Q. 15. http://www.irs.gov/uac/Section-7216-Frequently-Asked-Questions.
[28] Current Tax Return Disclosure Issues Involving Sec. 7216.
[29] *Id*.
[30] Return Preparer Penalties: A Comprehensive Review.
http://www.nysscpa.org/cpajournal/2001/0600/features/f063401.htm

must be available for inspection by the IRS. Under section 6695(d), the $25,000 maximum penalty for failure to comply with section 6107(b) applies per return period. This means that the IRS has the right to inspect either the returns prepared or a list of the tax preparer's clients' names and Social Security numbers.

Taxpayer Representation and Conflicts of Interest

"A CPA who provides auditing and other attestation services should be independent in fact and appearance. However, this standard does not apply to a practitioner under Circular 230 in the absence of any attestation service performed by a CPA or his or her firm for a client."[31] The issue raised by the AICPA Professional Standards occurs when a CPA provides both attestation services and tax services for the same client. If a conflict of interest is raised with a client for which the CPA provides both services. "Thus, CPAs providing such attestation services should consider (1) whether such engagement may materially limit the ability of such CPAs and their firms to provide federal tax advocacy services for the client under Section 10.29(a)(2), and (2) whether there is a significant risk that the representation of the client in federal tax advocacy matters will be materially limited by the personal interest of the practitioner or his or her firm due to the independence requirement of the attest engagement. … However, a practitioner may represent a client despite a conflict of interest if the practitioner reasonably believes he or she can provide competent and diligent representation to each affected client and if all affected clients waive the conflict by giving their written informed consent."[32]

HIPAA Privacy Issues & a Business Associate Agreement

Many accountants that audit the books of health care organizations see patient information. "They track treatment bills to follow the patient's co-pay, insurance payments, and write-offs, to see that the transactions were handled properly in the accounting system. This means that the accountant is a Business Associate." [33] A Business Associate must enter into a Business Associate Agreement and be both HIPAA and Texas H. B. 300 compliant.

"CPAs who have access to protected health information (PHI) are considered business associates regardless of whether that access comes directly from a covered entity, which may be your client, or through another third party (a business associate) of the covered entity. A business associate may be a CPA firm's client in an unrelated engagement. A CPA is considered a business associate if the CPA has access to PHI when performing duties and responsibilities, regardless of whether the CPA actually exercises this access." [34] Texas has more stringent compliance requirements under H.B. 300.

If you or your firm handles medical information, it may be a business associate under HIPAA

---

[31] *Conflicts of Interest: IRS Rules Differ from AICPA Professional Standards*. http://www.aicpa.org/publications/taxadviser/2011/november/pages/tpr_nov11.aspx.
[32] *Id*.
[33] *When is a Lawyer or Accountant aHIPAA Business Associate?* http://www.4medapproved.com/hitsecurity/lawyer-accountant-hipaa-business-associate/
[34] *Beware of Business Associate Agreements*. http://www.tscpa.com/content/59424.aspx.

regulations. It is mandatory that a business associate review the Business Associate Agreement and make sure it is HIPAA compliant and that any PHI is properly protected." The Privacy Rule requires a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), including reasonable safeguards to protect against any intentional or unintentional use or disclosure in violation of the Privacy Rule."[35] The Business Associate Agreement should address the reasonable safeguards and provide a description of the minimum safeguards.

Cloud computing and IT Security

About 94 percent of firms utilize smartphones for access to email, calendar and contacts, and 33 percent provide tablets or netbooks to senior management, according to the Association for Accounting Administration. It appears that most accountants rely on the Internet and smartphones for communicating with clients. That means that you are storing your emails, and their attachments, in the cloud. If the emails and their attachments are not encrypted, the information is easy to read by prying eyes. Therefore, if any emails contain personal information of a client, such information should be encrypted.

The problem with most professionals is that they don't know that most of their emails are stored in the cloud. As you sit here during the presentation reading your emails on your phone or tablet, the information you are looking at was just recently sent to you from some form of cloud storage. Was it encrypted? This is different than cloud computing. Cloud computing outsources accounting or IT functions. The AICPA has a webpage dedicate to Cloud Computing: http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/CLOUDCOMPUTING/Pages/default.aspx. This webpage provides an overview of Cloud Computing.

"To protect data confidentiality in the cloud, be prepared to negotiate specific contractual terms before uploading data into a cloud storage system. CPA firms should consider factors such as:

- Whether the provider will segregate your data;
- Whether the provider will access, use or copy data for its own purposes;
- Whether the provider will delete or return your firm's data at your request;
- How the provider will adequately purge data to ensure that confidential information is not compromised; and
- What the cloud provider's obligations are to notify your firm of a potential data breach.

CPA firms need to be concerned about security lapses in cloud data storage systems."[36] Many professionals are taking the position that they will only use the cloud as needed. Review the

[35] The HIPAA Privacy Rule in a Networked Environment Electronic Health Information Exchange. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf.

[36] Warning: Cloud Could Bring Storm. http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CPA/Feb/WarningCloud.jsp.

services used on the cloud, make sure there is an appropriate level of security, and encrypt any client's personal information. When you do use the cloud, make sure you choose the right level of security for the data you put there.

If you decide to utilize a Cloud Computing environment, it is necessary to receive assurances from the Cloud Service Provider (CSP) in the form of a Service Organization Control (SOC) assurance report. "Cloud customers that must meet PCI-DSS or HIPAA data protection requirements need assurance for a CSP's internal controls as they relate to security, confidentiality and privacy."[37] The real risk to the loss of data is the loss of reputation. If your firm loses your clients' data or personal information, you will have to inform your clients and many clients will move onto another CPA or firm. Protection of your client's data is really protection of your reputation.

IRS Use of Tax Preparer I.D. Numbers and its Supercomputer

There is a rumor on the Internet that the IRS has a new supercomputer that has access to social media going back to 2008. As well, the rumor is that the supercomputer can read all 200 million e-Filed returns in just 10 Hours.[38] The IRS is rumored to be using it new computer to locate audit targets. Regardless, as the IRS accumulates tax preparer identification numbers, PTINs, the IRS can then use its computer to look at how may EIC credits were taken by one tax return preparer or could look at how many educational credits a tax preparer put on the returns he or she prepared. It has been reported that the IRS has used the comparative analysis approach to find fraudulent tax return preparers improperly filing the earned income credit.[39] The IRS can now reverse engineer what type of work the tax return preparer is doing and if the deductions or credits look strange, then the IRS could review the return preparers work to see if the tax preparer is committing fraud by allowing all his or her clients to take fraudulent deductions. The IRS may now be auditing both the taxpayer as well as the tax return preparer.

William C. Nantz, CPA, CFF, CGMA, PTIN, MBA, JD, "Bill", provides is a Forensic Accounting Professor at HCC and provides forensic accounting services through William C. Nantz, CPA, a firm licensed as an accounting firm by the TSBPA. This presentation and the related article are provided as general information only and should not be construed as legal advice. This presentation and article are not intended to be applied to any particular situation as such application requires knowledge and analysis of the specific facts involved. Bill is also the founder of the Nantz Law Firm (the Nantz Law Firm is not a CPA firm) and Bill may be contacted at 713.542.5477 or bill@nantzlaw.com.

[37] The Growing Importance of Relevant Cloud Service Provider Assurance. http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CorpFin/ImportanceCloudServiceProviderAssurance.jsp.

[38] Protecting yourself from the New IRS's Big Brother Supercomputer. http://blog.intltaxcounselors.com/protecting-yourself-from-the-irss-big-brother-supercomputer/.

[39] IRS' approach to big data focuses on business outcomes. . http://www.federalnewsradio.com/534/3703560/IRS-approach-to-big-data-focuses-on-business-outcomes.