1-1-2002

AICPA member practice guide on the privacy protection provisions of the Gramm-Leach-Bliley Act and related Federal Trade Commission Regulations (Revised July 2, 2002)

American Institute of Certified Public Accountants. Tax Division. Privacy/Disclosure Task Force

AICPA MEMBER PRACTICE GUIDE ON THE PRIVACY PROTECTION PROVISIONS OF THE GRAMM-LEACH-BLILEY ACT AND RELATED FEDERAL TRADE COMMISSION REGULATIONS
(Revised July 2, 2002)

NOTE: Annual client notifications must begin before January 1, 2003.

Do the Requirements Apply to You?

The Gramm-Leach-Bliley Act and the related Federal Trade Commission (FTC) regulations contain restrictions on the disclosure of personal financial information of certain individual clients and also require the distribution of privacy notices to those clients. You are subject to these provisions if you are significantly engaged in providing individual clients with products or services for their personal, family, or household purposes (that is, for nonbusiness purposes) and those products or services fall within the law's very broad definition of "financial products or services". The term "financial products and services" includes tax return preparation and tax and financial planning, as well as many other activities. Therefore, if like many CPAs, you prepare individual tax returns or provide nonbusiness tax or financial planning advice, you are required to comply.

The AICPA sought an exemption from the notification requirements because of the stricter requirements of their members' enforceable Code of Professional Conduct, but the FTC determined that it did not have the authority to grant such an exemption because of the broad consumer protection language of the Gramm-Leach-Bliley Act. Similarly, the New York State Bar Association has sued the FTC, saying that its definition of "financial institution" should not include attorneys because of their professional responsibilities. The AICPA will seek legislative relief, but until there is a change in the law, CPAs must comply.

What is Required?

If you are subject to these provisions, you are required to provide notices regarding your privacy policy to the clients for whom you are providing the financial products or services. In addition, you are prohibited, with certain exceptions, from disclosing to a nonaffiliated third party any nonpublic personal information of the clients for whom you are providing the financial products or services. Several exceptions to the nondisclosure rule are likely to apply to practicing CPAs, such as those that permit disclosure:

1. to effect or administer the transaction requested by the client – for example, disclosure to a tax return processor for purposes of preparing the client's return;
2. to participate in a peer review; and,
3. to comply with federal, state, or local laws – for example, in response to a summons or subpoena.

In addition to the notice requirements, recently published FTC regulations require a written information security plan that describes your program to protect client information. All programs must be appropriate to your size and complexity, the nature and scope of activities, and the sensitivity of the client information at issue. You must:

1. designate the employee or employees to coordinate the safeguards,
2. identify and assess the risks to customer information in each relevant area of your operation, and evaluate the effectiveness of current safeguards for controlling these risks,
3. design a safeguards program, and detail the plans to monitor it,
4. select appropriate service providers and require them (by contract) to implement the safeguards, and
5. evaluate the program and explain adjustments in light of changes to your business arrangements or the results of security tests.

The new FTC regulations require special attention to the following areas that present special challenges and risks to information security: employee training and management; information systems, including network and software design, and information processing, storage, transmission, and retrieval; and security management, including prevention, detection and response to attacks, intrusions or other system failures.

CPAs protect confidential client information, and the new FTC regulations should not involve extra procedures, other than identifying an individual to coordinate safeguards, documenting your safeguard plans, and requiring service providers to implement safeguards. Because of the variety of situations that must be addressed, a model information security plan is not provided in this practice guide. The Safeguards Rule is available at www.ftc.gov.

When is it Required?

For new nonbusiness individual clients for whom you provide financial products and services, you must provide the initial notice no later than the acceptance of the client relationship. For these clients who are continuing, you must give the notice on an annual basis for continuing clients for whom a notice is required beginning in calendar 2002. In most cases, you should be able to accomplish this by including the notice with client billings or engagement letters. Thus, the first annual notice must be provided to continuing clients before January 1, 2003, and each subsequent annual notice must be provided within twelve months of that notice on a consistent basis each year.

What Will Be the Effect on Your Practice?

Other than the notice and information security plan requirements, being subject to these provisions should have no effect on your practice. As a CPA, you are already bound by your state ethics requirements. Also, AICPA members are bound by Ethics Rule 301 of the AICPA Code of Professional Conduct which is even more restrictive than the Gramm-Leach-Bliley/FTC provisions. Subject to certain exceptions, Rule 301 generally prohibits you from disclosing confidential client information without the specific consent of the client. In addition, subject to certain exceptions, Internal Revenue Code section 7216 makes it a misdemeanor for a paid income tax return preparer to disclose tax return information other than in connection with the preparation of the return.

What Sanctions are Provided?

The Gramm-Leach-Bliley Act refers to other financial institution legislation to provide penalties for noncompliance. While significant monetary penalties are possible, the FTC staff views these as targeted at abusive situations. Nonetheless, all CPAs subject to these provisions will want to be in compliance.

The Gramm-Leach-Bliley Act does not provide any new right of private action by clients, but CPAs continue have responsibilities under state privacy laws and under AICPA professional standards to protect client confidences.

What Should Be Included in the Privacy Notice?

The FTC regulations require that the notice be clear, conspicuous, accurate and in writing (or supplied electronically, with advance client approval). If the notice is to be combined with other information – e.g., engagement letters or tax return information organizers – the notice must have "distinctive type size, style, and graphic devices, such as shading or sidebars."

The notice must contain the following information:

1. The types of nonpublic personal information you collect regarding the client;
2. The types of nonpublic personal information you disclose about the client;

3. The parties to whom you disclose this information, other than under an exception to the prohibition on nondisclosure;
4. The client's right to "opt out" of the disclosure (generally not applicable to CPA clients because CPAs normally do not disclose client information);
5. Your policies with respect to sharing information on a person who is no longer a client, and
6. Your practices for protecting the confidentiality and security of your clients' nonpublic personal information.

A sample privacy notice is attached for your reference.

Special Practice Issues, Business and Industry Applications and Additional Information.

The above discussion and the attached sample disclosure statement are intended to serve most CPAs in practice. They do not contemplate certain special practitioner situations, such as joint marketing activities (with law firms, for example) and international services. Also, because of the myriad of possible types of businesses and activities, this practice guide is not intended to provide guidance to members in business and industry. For CPAs wishing additional information, those having special situations, or members in business and industry, there is an excellent outline of the FTC regulations at its website, http://www.ftc.gov/privacy/glbact/glboutline.htm (in hypertext markup language format) or http://www.ftc.gov/privacy/glbact/glboutline.pdf (in portable document format (looks better, but requires Adobe Acrobat software)). You can find additional helpful information, including the FTC regulations and frequently asked questions, at the FTC website—go to www.ftc.gov and at the bottom of the page, click on Gramm-Leach-Bliley Act for a list of documents and information.

****

This practice guide was prepared by the AICPA Tax Division's Privacy/Disclosure Task Force which included members from the Personal Financial Planning Committee and PCPS:

Members
Tom Ochsenschlager, Chair
Peter Golotko
Janice Johnson
Dan Mendelson
Jean Trompeter
Robert Warren

Staff
Gerald Padwe
William Stromsem
Peter Kravitz

****

SAMPLE DISCLOSURE NOTICE

(Insert Your Firm Name) Privacy Policy

CPAs, like all providers of personal financial services, are now required by law to inform their clients of their policies regarding privacy of client information. CPAs have been and continue to be bound by professional standards of confidentiality that are even more stringent than those required by law. Therefore, we have always protected your right to privacy.

Types of Nonpublic Personal Information We Collect

We collect nonpublic personal information about you that is provided to us by you or obtained by us from third parties with your authorization.

Parties to Whom We Disclose Information

For current and former clients, we do not disclose any nonpublic personal information obtained in the course of our practice except as required or permitted by law. Permitted disclosures include, for instance, providing information to our employees, and in limited situations, to unrelated third parties who need to know that information to assist us in providing services to you. In all such situations, we stress the confidential nature of information being shared.

Protecting the Confidentiality and Security of Current and Former Clients' Information

We retain records relating to professional services that we provide so that we are better able to assist you with your professional needs and, in some cases, to comply with professional guidelines. In order to guard your nonpublic personal information, we maintain physical, electronic, and procedural safeguards that comply with our professional standards.

****

Please call if you have any questions, because your privacy, our professional ethics, and the ability to provide you with quality financial services are very important to us.

FREQUENTLY ASKED QUESTIONS

1. I'm a professional CPA and have a duty of client confidentiality that is stricter and carries more sanctions than the Gramm-Leach-Bliley Act. I am concerned that this notification may confuse my clients because it makes no sense to notify them that I am doing what they always have trusted me to do. Are you sure I have to do this?

Yes. The Gramm-Leach-Bliley Act places requirements on those who are "significantly engaged" in providing individual clients with tax return preparation and tax and financial planning services, including CPAs. While you are already protecting client confidentiality under Rule 301 of the AICPA Code of Professional Conduct, Gramm-Leach-Bliley also requires you to notify clients of your policies to protect the privacy of their personal financial information, as described in the practice guide. Although the AICPA will continue working for a regulatory or legislative exemption for CPAs, the current law requires you to comply.

2. Do I have to provide the privacy notification to clients who are minors, such as children of clients for whom I do individual tax returns?

The regulations do not address this issue, and generally minors are protected by Gramm-Leach-Bliley. However, minors in a family do not have to receive separate notifications where the parent is, in fact, the consumer. The notice would be sent to the parent who provides the personal financial information for the children, and is thus the customer or client, even if the child is a college student.

3. Do I have to provide separate notifications to both spouses?

Section 313.9(g) of the regulations states that where there are joint account holders, a single privacy notice can be provided, and this would apply where there is a joint income tax return. However, where separate personal financial services are provided to each spouse or where both spouses request separate notices, separate notifications are required.

4. I provide services to a trust—do I need to provide a privacy notification to the trustee or the beneficiaries or both?

This is a difficult issue because a trust can be both an entity and an aggregate from a theoretical standpoint. The preamble to the regulations exempts trustees from providing notices to beneficiaries, but this is at least partly because trustees are fiduciaries with responsibilities to the beneficiaries, and this provides protection. Also, Gramm-Leach-Bliley is intended to protect individuals, not trusts, and in most cases, notification to trustees and beneficiaries would not be required. However, if you are providing tax, investment advisory services, trust accounting, and other financial services to a trust, but these flow through directly to individual beneficiaries through the trust with whom you work closely, you should consider who the real recipient of your services is and whether you should provide notification to beneficiaries.

5. Same question as 4, but with respect to partnerships.

Same answer as 4. In most situations, partnerships would not receive notification, as they are businesses, not individuals which are the focus of Gramm-Leach-Bliley. However, if you are providing financial services through a partnership to individual partners with whom you work closely, you should consider who the real recipient of your services is and whether you should provide notification to partners.

6. Are there any state privacy protection laws that I have to comply with?

Our practice guide addresses the Federal Gramm-Leach-Bliley Act, and does not address state privacy statutes, regulations, or cases. If there are additional state requirements for privacy protection, these are best addressed by your state society. If you are a state-registered investment advisor, for instance, you must also comply with the state requirements for investment advisors.

7. I may be selling or merging my firm in the near future—do I have to notify my clients that I may disclose personal financial information to the new/additional owners and give them an opportunity to opt out of this disclosure?

Section 313.15 (a)(6) of the FTC regulations provide an exception to the requirement for client notice and "opt-out" provisions "in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit."

However, be aware that Section 7216 of the Internal Revenue Code prohibits the unauthorized disclosure of tax return information, and while there are some exceptions for sales and mergers under the Treasury Regulations, the extent of these exceptions is not clear. Section 301.7216-2(l) and (m) allows the disclosure of a list of tax clients, which would normally be tax return information, in conjunction with a sale or disposition of the practice. Also, where a practice is transferred in steps, such as where a new owner joins the firm, and then the old owner leaves, Regulations Section 301.7216-2(e)(1) does not require client permission for turning over tax return information. The IRS is currently revising the Section 7216 regulations, and in the meantime, because of potential criminal sanctions and in the interest of maintaining good client relations, it might be wise to obtain permission from clients before turning over tax returns or return information in a sale or merger. Also, the AICPA Code of Professional Conduct protects client confidentiality in a merger or acquisition. Specifically, AICPA Interpretation 301-3 [ET section 301.04] requires that a member take appropriate precautions (for example, through a written confidentiality agreement) so that the prospective new owners do not disclose any information obtained during the course of the review of the member's practice. Members reviewing the practice in connection with a prospective purchase or merger are also bound by Rule 301 – Confidential Client Information.

After the sale or merger, the new firm must notify clients if the privacy policies will change—see FTC regulations section 313.4(e)(1)(i).

8. In auditing a financial institution, I have been asked by the client to sign a Gramm-Leach-Bliley motivated agreement not to disclose any personal financial information about the institution's clients that I learn in the audit. Some information in my records may be disclosed in a peer review. Do I have to sign such an agreement?

Gramm-Leach-Bliley allows financial institutions to disclose information to auditors without notifying clients or giving them an opportunity to opt out of disclosure. Similarly, in a peer review CPA firms can disclose, without a client opt-out, information on their personal financial service clients. Also, peer reviews are to be conducted in a way that protects CPA client confidences, so the public is protected. However, while Gramm-Leach-Bliley does not require such an agreement, if the client or the client's attorney require the CPA to sign a non-disclosure agreement as part of the audit engagement, the CPA should require that the agreement allow disclosure to a peer reviewer to avoid breaching the agreement in fulfilling peer review requirements.

9. Are there agencies other than the FTC who have regulations under Gramm-Leach-Bliley that apply to me?

Other agencies, like Federal banking agencies and the SEC, also have regulatory authority under Gramm-Leach-Bliley. However, the FTC's regulations, discussed in our practice guide, apply to the broadest array of financial services, and other agency regulations are consistent with them. For SEC regulated entities, like federally registered investment advisers, SEC Regulation S-P imposes requirements that are similar to the FTC, and the SEC regulations are available at www.sec.gov/rules/final/34-42974.htm

10. How can I reduce the cost of mailing this notice to my clients--can I put other client communications in the same envelope to try to get some value for this effort and expense?

The notification can be included with your engagement letter, client organizer, or even a client newsletter. Your client notification must be "prominent," but that doesn't mean that you can't put other client communications in the same envelope.

11. Where can I get a copy of the Gramm-Leach-Bliley Act and FTC regulations?

The Act is at http://www.currentlegal.com/LegalNews/uspl1998/106-102.html and the regulations and additional practice guidance are at: www.ftc.gov/privacy/index.html (then scroll down to the Gramm-Leach-Bliley Act).

12. Do I have to personalize the privacy notification letters to my clients and keep copies of all the letters to prove that I sent them?

You don't have to send a personalized letter to each client—you can send a standardized "Dear Client" letter or could even include the notice in a client newsletter (the notification must be prominent) sent to each individual client. If you make a good-faith effort and are in substantial compliance, it is extremely unlikely that you will ever have to "prove" that you sent the notices. However, you should maintain a simple record of the mailing—a copy of the letter and a list of the clients to whom it was sent (or at least a description of the categories of clients to whom it was sent). A written office procedure indicating that the notice is to be mailed to new clients, and annually to continuing clients would also help show compliance.

13. I am the sole shareholder in both my CPA firm and a separate financial planning firm (insurance or stock brokers), and would like to "share" information between the two businesses. Do I have to notify the clients of each practice that I plan to disclose information to the other? Does the answer change if the financial planning firm has some additional non-CPA owners?

Where the separate financial services practice is wholly owned by the CPA firm, there is no need to notify clients of either firm that you plan to share information with the other, and there is no need to inform them that they can "opt out" of such disclosure. Disclosure of CPA client information to others (non-CPA owners of the financial services firm or disclosure to others by the separate financial services firm) would require notification and opt-out language, and there are examples of this language in the regulations (see answer to Question 12). Caution—the disclosures in the preceding sentence might also violate the CPA's duty of client confidentiality or, if tax return information is disclosed, might be a criminal misdemeanor under Internal Revenue Code Section 7216.

14. What steps must I take to comply with the FTC Safeguards Rule?

In general, (1) you must identify an individual employee who will coordinate safeguarding of client records, (2) develop a written plan for information security, and (3) review service provider arrangements to be sure that the security of client financial information is safeguarded.

15. (From FTC Website) I am a tax return preparer and I understand that I may be subject to the Privacy Rule concerning the disclosure of my clients' nonpublic personal information. However, I also am subject to section 7216 of the Internal Revenue Code, which restricts the use and disclosure of my customers' federal tax return information. Do the privacy provisions of the GLB Act and the Privacy Rule supersede the restrictions in section 7216? May I now disclose my customers' federal income tax return information after I provide them with the proper notices and give my customers a reasonable opportunity to opt out?

The Privacy Rule does not supersede the restrictions in section 7216. The GLB Act and the Agencies' implementing regulations do not authorize a financial institution to disclose nonpublic personal information in a way that is prohibited by some other law. Therefore, you may not avoid the restrictions of section 7216 by providing your customers with an opt out notice and a reasonable opportunity to opt out.