

The following article will be published in the March issue of the Journal of Accountancy

Legal and Ethical Considerations Regarding Outsourcing

By Richard I. Miller and Alan W. Anderson, CPA

AICPA members have responsibilities related to the practice of using third parties to provide services in engagements for clients. Primary among them are security and confidentiality of information, due professional care and compliance with provisions of the Code of Professional Conduct. In addition, members must monitor security procedures that third-party providers have put into place to ensure they remain effective.

The Institute has received a number of inquiries regarding the responsibilities of members who use third-party service providers in client engagements. Commonly known as “outsourcing,” this practice has been employed by members for decades to provide more effective services to their clients. Examples of services that may be outsourced include

- Tax preparation and processing.
- Bookkeeping.
- Certain audit procedures performed by contract staff.
- Outside specialist services in connection with an audit.
- Human resources services.
- Investment advisory services.
- Workpaper storage or destruction services.

This paper will discuss member responsibilities in three areas: AICPA ethical standards, the Gramm-Leach-Bliley Act (GLBA) and certain Internal Revenue Code provisions.

AICPA ETHICAL STANDARDS

The AICPA's professional ethics division addressed the use of third-party providers as early as 1973 in Ethics Ruling no. 1, under the AICPA Code of Professional Conduct, Rule 301, Computer Processing of Client Returns (ET section 391.001-.002). While that ethics ruling specifically deals with using outside services to process tax returns, it also would apply to any use of third-party providers. The ruling advises that members "must take all necessary precautions to be sure the use of outside services does not result in the release of confidential information." (Because of continuing questions concerning the use of third-party providers, the professional ethics executive committee [PEEC] in its meeting on January 22, 2004, appointed a task force to study whether this ruling needs to be revised. Should any further guidance be issued by the PEEC, it will be made available to members as soon as practicable.)

The code also states that a member remains responsible for ensuring the accuracy and completeness of the services provided by the third-party provider. Specifically, it requires all professional services to be performed with professional competence and due professional care (see Rule 201, General Standards [ET section 201.01]). Accordingly, using third-party providers to assist in performing services for clients does not in any way excuse practitioners from these or other responsibilities under the code.

In view of these requirements, members should satisfy themselves regarding the competence, practices and procedures of any third-party provider, regardless of the type

of services provided or the location at which they are performed. At a minimum, it seems advisable for members to discuss with the third party the specific controls in place to safeguard the client's information and to satisfy themselves that such controls are adequate. For example, where client information is transmitted via the Internet, the member may want to inquire as to specific security measures in place, such as

- Encryption techniques.
- The use of private leased lines or virtual private networking connections with authorized users.
- The availability and processing integrity of the information.
- Whether the third-party provider has had an engagement performed (internal or external) on the security of their systems.
- Whether the third-party provider has obtained an independent security attestation regarding their systems.

Once satisfied there are sufficient procedures in place to ensure the security of information transmitted electronically to a third-party provider, members also should satisfy themselves that controls are in place to ensure the information remains confidential. There are many ways by which third-party providers might satisfy a practitioner in this regard. For example, they may use nondisclosure agreements with their employees; implement certain computer protections that prohibit downloading, printing, scanning or copying a client's financial information; and incorporate firewall security to prevent outsiders from hacking into the system. Periodic testing of these security measures could also provide more comfort to the practitioner. Whatever the measures used by the third-party provider, the member should be satisfied that reasonable

efforts are undertaken to assure the confidentiality of the information to which the provider has access. A confidentiality breach by the outsourcer, even if all of the above steps were taken, still will be the responsibility of the member. (The subjects of security, privacy, confidentiality, online processing and availability, among others, are covered in the AICPA/CICA Trust Services Principles and Criteria Framework, available at www.aicpa.org/trustservices).

As part of their overall responsibility to ensure that all professional services are performed with professional competence and due professional care, members are responsible for adequate supervision of all such professional services. The member should review all work performed by a third-party provider since he or she will remain fully responsible for the accuracy and completeness of the services provided.

Should a question be raised regarding a member's compliance with any of his or her professional responsibilities, including those discussed above, the member may be in a better position if he or she can demonstrate that he or she took reasonable steps to meet those obligations.

The code does not require members to advise clients regarding their use of a third-party provider. Therefore, advising the client of such use is at the sole discretion of the member unless the client questions the member regarding such practice. However, whether or not clients are advised of the use of third-party providers, members are not relieved of their responsibilities to comply with the code as outlined above.

GRAMM-LEACH-BLILEY ACT

In addition to the member's responsibilities under the code to maintain confidentiality, the Gramm-Leach-Bliley Act of 1999 needs to be considered as well. In GLBA, Congress included protections that allowed consumers to determine when personal financial information could be shared among financial service institutions. The Federal Trade Commission (FTC), one of the federal agencies charged with implementing the privacy requirements of the GLBA, promulgated a set of rules that govern the use of consumer financial information

(www.ftc.gov/privacy/privacyinitiatives/financial_rule_lr.html).

These rules, particularly 16 CFR [Code of Federal Regulations] section 313.4, require persons or businesses offering financial services for personal, family or household purposes to provide notices regarding their information-sharing policies and practices. The notices must be provided to ongoing customers at the time the customer relationship begins and, according to 16 CFR section 313.5, annually thereafter. A person who provides personal, nonpublic information to obtain financial, investment or economic advisory services, regardless of whether there is a continuing customer relationship, is also entitled to notice prior to, and the ability to opt out of, any actual disclosure of such information to a nonaffiliated third party. Therefore, as currently interpreted, GLBA requires practitioners who provide, among other things, tax planning and tax preparation services to individual clients, to give notice of the practitioner's policy regarding disclosure of private information at the start of an engagement, and annually thereafter.

The notices required by GLBA generally require disclosure to the client of categories of nonaffiliated third parties to whom there is disclosure of nonpublic information, under section 313.6. GLBA does not, however, require that a practitioner

specifically disclose to a client the fact that independent third-party providers are used in performing services for clients. Section 313.14 provides an exception to the notice and opt-out requirements for “processing and servicing transactions.” In summary, the notice and opt-out requirements described above do not apply if (1) the practitioner shares nonpublic personal information in connection with servicing or processing a financial product or service that a consumer requests or authorizes or (2) the sharing of information with the third party is required, or is a usual, appropriate or acceptable method to carry out the transaction or service of which the transaction is a part, or to record, service or maintain the consumer’s account in the ordinary course of providing the financial service or product.

In other words, if the third-party provider is connected to or involved in the provision (or processing) of the services offered by the practitioner, there is no requirement to disclose to the client the fact that information is shared with that third party. Accordingly, if you disclose only to nonaffiliated third parties covered by the exceptions described above, the FTC, in section 313.6 and its “Sample Clauses” (in appendix A), states the following language must be placed in the notices: “We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.” If you disclose to nonaffiliated third parties that are not covered by the exceptions, then you are required to list in your notices, by category, the nonexempt third parties (such as insurance agents, retailers or marketers), and the FTC states the following clause should also be added: “We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.”

The FTC's rules do, however, limit the extent to which a nonaffiliated third party may use and reuse the information that has been disclosed. Specifically, a nonaffiliated third party may disclose the information only to the financial institution itself, the third party's affiliates (who are also bound by the same restrictions as the third party) or pursuant to the exceptions outlined above—that is, to obtain a service in connection with the service or the function the outside firm is performing.

Furthermore, the FTC promulgated safeguard rules that require a financial institution, which, again, could be anyone offering financial services, to oversee the third-party provider's use of the information and ensure compliance with GLBA. This rule (16 CFR section 314.4) requires that institutions develop, implement and maintain an information security program. In doing so, an institution must oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards. (AICPA/CICA Trust Services Principles and Criteria Framework may be useful as a benchmark when determining the appropriate safeguards for service providers.)

INTERNAL REVENUE CODE

IRC section 7216 prohibits anyone who is involved in the preparation of tax returns from knowingly or recklessly disclosing or using the tax-related information provided other than in connection with the preparation of such returns. Anyone who violates this provision may be subject to a fine or even imprisonment. The regulations under section 7216 provide an exemption from this law for tax return preparers who disclose taxpayer

information to a third party for the purpose of having that third party process the return. Nevertheless, members should make third-party providers to which they have supplied protected client information aware of this requirement. Note there is no requirement in section 7216 or its regulations for a member to inform the client that a third-party provider is being used.

In addition, IRC section 7525 provides a client with a privilege similar to an attorney-client privilege when they make certain tax-related disclosures to, among others, CPAs. Care needs to be taken to assure that a third-party provider does not do anything that adversely affects a client's rights under this provision.

Because of the requirements of federal law as outlined above, it is important for practitioners to be aware of their continuing obligations to safeguard client data. In this regard, it would be advisable—indeed likely necessary—to perform due diligence before disclosing information to a third-party provider to ensure the provider is capable of adequately protecting nonpublic information. (As noted earlier, the Code of Professional Conduct imposes similar obligations.) This seems particularly imperative where the provider is located in an unfamiliar location, or where enforcement of privacy laws and the prosecution of those who misappropriate private information may be more difficult. Thus, the contract between the practitioner and the third-party provider should contain appropriate provisions for the protection of consumer privacy.

THE PRACTITIONER'S DUTY

Whether they derive the regulations from the Code of Professional Conduct, the Internal

Revenue Code or the Gramm-Leach-Bliley Act, practitioners and their firms are responsible for maintaining the security and confidentiality of client information. In addition, in performing any service for a client, practitioners must do so with professional competence, with due professional care and in compliance with all provisions of the Code of Professional Conduct. Even after the practitioner is satisfied that a third-party provider is properly structured to ensure continued compliance with all laws and regulations and ethical requirements, a practitioner's duties do not end. Monitoring procedures should be established to ensure the procedures that third-party providers have put into place remain effective.

Practitioners and their firms should consult their own legal advisers for additional guidance on this subject.

Copyright © 2004, American Institute of Certified Public Accountants, Inc.

RICHARD I. MILLER is general counsel and secretary of the AICPA. His e-mail address is rmiller@aicpa.org. ALAN W. ANDERSON, CPA, is senior vice-president of member and public interests at the AICPA. His e-mail address is aanderson@aicpa.org.

Executive Summary

- **THE AICPA HAS RECEIVED A NUMBER** of inquiries regarding practitioners' responsibilities in outsourcing engagements. The applicable guidance is found in the AICPA's Code of Professional Conduct, the Gramm-Leach-Bliley Act and certain Internal Revenue Code provisions.
- **THE CODE OF PROFESSIONAL CONDUCT STATES** that a member remains responsible for ensuring the accuracy and completeness of the services rendered by the third-party provider.
- **MEMBERS SHOULD SATISFY THEMSELVES** regarding the competence, practices and procedures of any third-party provider, regardless of the type of services provided or the location at which they are performed. At a minimum, it seems advisable for members to discuss with the third party the specific controls in place to safeguard the client's information and to satisfy themselves such controls are adequate.
- **WHATEVER THE MEASURES USED BY THE** third-party provider, the member should be satisfied that reasonable efforts are undertaken to assure the confidentiality of the information to which the provider has access. A confidentiality breach by the outsourcer, even if all of the noted steps were taken, will still be the responsibility of the member.
- **THE CODE OF PROFESSIONAL CONDUCT DOES NOT** require members to advise clients regarding their use of a third-party provider. Such disclosure is at the sole discretion of the practitioner. Advising clients of the use of third-party

providers, however, in no way relieves members of their responsibilities to comply with the code as discussed in the article.