

## Protecting Client Information Obtained During An Audit

There has been widespread concern regarding the way CPA firms are protecting client data. This is understandable because of the upsurge in publicity generated by security breaches at financial services firms. In addition, with the increased use of internet activity for transmitting and storing data, privacy issues are paramount. Protecting client data is not an optional business practice. Rule 301 of the AICPA Code of Professional Conduct *Confidential Client Information* provides that a member in public practice shall not disclose any confidential client information without the client's specific consent. Confidentiality requirements are also mentioned in the NCUA regulations as well as in the Gramm-Leach-Bliley Act (GLBA). Presently, CPA firms are now exempt from sending their clients an annual privacy notice as previously required by the GLBA. This was made possible because CPAs are certified or licensed by state boards of accountancy and are already subject to state laws and regulations that prohibit disclosure of nonpublic personal information without the express consent of the client. However, CPAs are required to follow more rigid professional standards than those required by law. In doing so, protecting client information has always been an important concern for CPA firms.

**“...protecting client information has always been an important concern for CPA firms.”**

Credit unions should look to the CPA firm's privacy policy to address any concerns on the methods used to protect client privacy. The privacy policy could be part of the contract with the CPA firm or a stand-alone document. This policy should define the types of information that the firm will collect. A privacy policy may state that the firm will collect nonpublic personal information that is either provided by the credit union or obtained by them with your authorization. Any nonpublic personal information obtained in the course of

the audit should not be disclosed unless permitted or required by law. For example, employees of the CPA firm will need access to sensitive credit union data in order to perform their tasks. Unrelated third parties may need to know certain information in order to assist in providing services to the credit union. One example is sending out a request to confirm the existence and balance of an account that the credit union has as of the audit date.

There may be instances when CPA firms will need to make their audit workpapers available to the examiners as required by state regulatory agencies and/or NCUA Regulation 715.10(b). At Nearman, Maynard, Vallez, whenever our workpapers are provided to the examiners, we will include a letter stating that these workpapers are made available under the condition that they are exempt from disclosure under the Freedom Information Act, because they are designated as trade secrets and confidential commercial and financial information pursuant to the Code of Federal Regulations. This requirement prevents anyone in the federal government from gaining access to the workpapers, which contain sensitive credit union information, without our written permission. In doing so, all information within our workpapers is protected from unauthorized use when not in our possession.

CPA firms are periodically subject to peer review. The GLBA allows credit unions to disclose information to auditors without notifying members or giving them an opportunity to opt out of disclosure. Similarly, during a peer review, CPA firms can disclose information on their clients without a client opt-out. However, peer reviews are conducted in a way that protects CPA client confidences so that members are protected.

The privacy policy should address protecting the confidentiality of current and former client information. It should state the security measures it employs to ensure credit union information is used only by employees that need to have access to this information. Credit union

data should be retained only as intended to comply with professional guidelines and to service the needs of the credit union. Sensitive data that is no longer needed should be destroyed or disposed of in accordance with NCUA regulations. At Nearman, Maynard, Vallez, we routinely shred sensitive papers and destroy or erase electronic media so that information cannot be read or reconstructed.



**“The safeguarding of sensitive credit union information is best achieved by following a comprehensive privacy policy.”**

CPA employees should have a background security check before being hired. Once hired, they should be trained on the firm's policies and procedures pertaining to safeguarding credit union information obtained during an audit. This will enable employees to be more aware of their specific responsibilities when obtaining sensitive data for an audit. As part of our quality control review, we routinely check to ensure our employees are using proper methods for obtaining and securing credit union information.

Protecting credit union information obtained during an audit has always been an important concern and is a professional and legal responsibility of CPA firms. The safeguarding of sensitive credit union information is best achieved by following a comprehensive privacy policy. This should include physical, electronic, and procedural safeguards to provide reasonable assurance that credit union information is protected. Proper procedures should be routinely monitored for compliance as part of the firm's quality control. ♦

Nicole Lee, MPA, Senior Auditor

**Nearman, Maynard, Vallez, CPAs & Consultants, P.A.**

Atlanta: 205 Brandywine Blvd., Suite 100, Fayetteville, GA 30214-1561. (770) 461-5706. FAX (770) 719-1888

Miami: 10621 North Kendall Dr., Suite 219, Miami, FL 33176. (305) 598-1730. FAX (305) 595-9316

Toll Free: (800) 288-0293 Website: [www.nearman.com](http://www.nearman.com) E-Mail: [info@nearman.com](mailto:info@nearman.com)