THE TAXBOOK News Release Date: 8/6/2018

Safeguards Rule

Cross References

• www.ftc.gov

Tax professionals are included in the types of businesses that are required to comply with the Safeguards Rule. Under these rules, financial institutions are required to protect the consumer information they collect. Tax preparers are considered financial institutions for purposes of these rules. The IRS recently reminded the tax preparation community of the responsibility to safeguard client information, including the use of strong passwords, the use of antivirus software, firewalls, two-factor authentication, backup software/services, drive encryption, and data security plans.

Tax professionals are also required to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of this written plan, a tax professional must:

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

If a tax professional has employees, the Safeguards Rule requires the tax professional to implement employee management and training. The tax professional should consider:

- Checking references or doing background checks before hiring employees who will have access to customer information.
- Asking every new employee to sign an agreement to follow the tax preparation firm's confidentiality and security standards for handling customer information.
- Limiting access to customer information to employees who have a business reason to see it.
- Controlling access to sensitive information by requiring employees to use strong passwords that must be changed on a regular basis. Passwords should be at least six characters, upper-and lower-case letters, and a combination of letters, numbers, and symbols.
- Using password-activated screen savers to lock employee computers after a period of inactivity.
- Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. Employees should store these devices in a secure place when not in use.

- Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
  - Locking rooms and file cabinets where records are kept,
  - Not sharing or openly posting employee passwords in work areas,
  - Encrypting sensitive customer information when it is transmitted electronically via public networks,
  - Referring calls or other requests for customer information to designated individuals who have been trained in how the tax preparation firm safeguards personal date, and
  - Reporting suspicious attempts to obtain customer information to designated personnel.
- Regularly reminding all employees of the tax preparation firm's policy and the legal requirement to keep customer information secure and confidential.
- Developing policies for employees who telecommute. Consider whether or how employees should be allowed to keep or access customer data at home. Require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
- Imposing disciplinary measures for security policy violations.
- Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

All tax professionals, whether they have employees or not, should maintain security throughout the life cycle of customer information.

- Know where sensitive customer information is stored and store it securely. For example, records must be stored in a room or cabinet that is locked when unattended. Customer information stored on a server or computer must have strong passwords. Such computers must also be kept in a physically-secure area. Backups and archives should be stored off-line in a physically-secure area. Maintain a careful inventory of the tax preparation firm's computers and any other equipment on which customer information may be stored.
- Take steps to ensure the secure transmission of customer information.
- Dispose of customer information in a secure way.
- Monitor the websites of software vendors and read relevant industry publications for news about emerging threats and available defenses.
- Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information, such as getting the latest computer software patches that resolve software vulnerabilities, use of anti-virus and anti-spyware software, maintaining up-to-date firewalls, etc.

Author's Comment

This includes all software used on a computer that contains customer information which is connected to the internet, such as allowing Windows 10 to update itself when it wants to. Storing customer data on a computer connected to the internet that is running Windows XP, which is no longer supported or updated for the latest threats is a violation of the Safeguards Rule.

For more information, go to www.ftc.gov/privacy/glbact