Gramm-Leach-Bliley Act 'Safeguards Rule' Checklist

The amended Safeguard Rule will go into effect on October 27th, 2022. Each item, presented in question form, highlights a feature of the amended Safeguard Rule that investment managers should consider when building information security plans.

Information Security Plan Considerations

- Do you have one or more qualified individuals responsible for the firm's information security program?
- Do you train security personnel and verify that they take steps to maintain current knowledge of cybersecurity best practices?
- Does your information security plan require periodic reports about information security to the board of directors or governing body of the firm at least annually?
- Does your information security plan include policies and procedures detailing when and how records containing consumers' nonpublic personal information (NPI) should be kept, accessed, or transported off your business premises?
- Do you require multi-factor authentication for device containing NPI?
- Do you have a written incident response plan?
- Do you have a procedure for documenting any action taken in connection with any breach of security, and does that procedure require incident review of events and actions taken to improve security?
- Have you identified the paper, electronic and other records, computing systems and storage media, including laptops and portable devices that contain personal information?
- Does your information security plan include data inventory and classification?
- Have you identified and evaluated reasonably foreseeable internal and external risks to the paper and electronic records containing NPI?
- Does the information security plan continuously monitor, annually perform penetration testing, and biannual vulnerability scans?
- Does the information security plan include regular ongoing employee training and procedures for monitoring employee compliance?
- Does the information security plan encrypt NPI?
- Do you have secure testing practices for 3rd party services?
- Do you, to the extent feasible, oversee service providers by selecting ones capable of maintaining appropriate safeguards and requiring them by contract to maintain those safeguards?

- Do you have procedures in place for safely disposing customer data?
- Do you have policies and procedures for monitoring the activity of authorized users?
- Do you maintain an internal assessment that evaluates identified security risks, the quality of controls that are currently in place, and an explanation of how these risks can be mitigated?

This checklist is not substitute for compliance with the amended Safeguard Rule or legal advice.

To learn more, contact me at E: info@appolocompliance.com | P: 332-910-8302 |or visit me at Appolocompliance.com