Gramm-Leach-Bliley Act (GLBA Compliance Checklist)

Scope of Regulation	Yes/No or NA	Comments
1. Is the organization considered a financial institution under GLBA (Gramm-Leach-Bliley Act)? • **Note**: Under GLBA, an organization must be significantly engaged in financial activities to be considered a financial institution. • **Examples of financial institutions:** Mortgage lender or broker; check casher; pay-day lender; credit counseling service; financial advisers; medical service providers with long-term payment plans that involve interest charges; tax planning and preparation services; auto dealers that lease or finance; collection agency services; relocation services that assist with financing or mortgages; the sale of money orders/savings bonds/traveler's checks; and collection agency, real estate appraising, or government entities that provide financial products. • **Examples of financial activities:** Lending, exchanging, transferring, investing for others, or safeguarding money or securities; insuring against loss, harm, damage, disability, or death; and providing financial advisory services, extending credit, or servicing loans.		
2. Does the organization provide a financial product or service to customers?		
3. Does the organization provide an initial privacy notice not later than when the customer relationship is established?		
4. Does the organization provide an opt-out notice before sharing nonpublic personal information with nonaffiliated third parties? a. Provide customers a "reasonable opportunity to opt-out" (e.g., 30 days from the date the notice is mailed) • **Note**: An organization may disclose nonpublic personal information to nonaffiliated third parties under several exceptions where the customers do not have the right to opt-out (e.g., third-party provider services for the organization and other financial organizations with which the organization entered into a joint marketing agreement).		

5. Does the organization provide an annual privacy notice to its customers?		
6. Does the organization provide new revised privacy and opt-out notices when it changes privacy practices?		
7. Is the notice: a. Clear and conspicuous? b. Reasonably understandable?		
8. Does the initial and annual notice contain: a. Categories of nonpublic personal information collected? b. Categories of nonpublic personal information disclosed? c. Categories of affiliates and nonaffiliated third parties to whom nonpublic personal information is disclosed? d. Information on whether the organization discloses nonpublic personal information about former customers? e. An explanation of the customer's right to opt-out? f. Disclosures required by the Fair Credit Reporting Act? g. The policies and practices with respect to protecting the confidentiality and security of nonpublic personal information?		
9. Does the opt-out notice contain: a. A statement that nonpublic personal information is disclosed to nonaffiliated parties? b. The consumer's right to opt-out of those disclosures? c. A description by which the consumer can opt-out?		
10. Does the organization have a written information security program? a. Is it implemented? b. Is it maintained? c. Is someone responsible for coordinating the security program? d. Has the organization completed a risk assessment of the security, confidentiality, and integrity of customer information?		

Effective: Privacy Rule—Nov. 13, 2000. Compliance by July 1, 2001. Safeguard Rule—May 23, 2003

Source:

Federal Register: Part III Federal Trade Commission 16 CFR part 313, Privacy of Consumer Financial Information; Final Rule, May 24, 2000.
Federal Register: Part VII Federal Trade Commission 16 CFR Part 314 Standards for Safeguarding Customer Information; Final Rule, May 23, 2002.

Enforcement: Federal Trade Commission