

**OCC Guidelines: Relaxed Standards for Monitoring Law Firm Service Providers**

* Pursuant to the 2001 OCC Interagency Guidelines Establishing Information Security Standards (“OCC Guidelines”), every regulated Financial Institution must “exercise an appropriate level of oversight over each of its service providers.”
* Financial Institutions are granted **great flexibility** with regard to this oversight, and are encouraged to individualize the monitoring process based on the particular characteristics of each service provider. For example, the OCC Guidelines note that some service providers “**may already be subject to legal and professional standards** that require them to safeguard the [Financial Institution’s] customer information.” Financial Institutions are encouraged to “do a risk assessment” to “determine for themselves which service providers will need to be monitored.”
* Law firms, as a key service provider to Financial Institutions, are already subject to a variety of legal and professional standards that require them to safeguard the Financial Institutions’ customer information. Accordingly, Financial Institutions do not need to monitor law firm service providers with the same level of stringency as other service providers.

**Legal Standards**:

Law firms are subject to the highest legal standards. Laws requiring the safeguarding of customer information include:

* **Gramm-Leach-Bliley Act**: There is no exception in the GLB Act for law firms. Consequently, a law firm that is significantly engaged in one or more of the financial activities listed in the Act’s regulations, including real estate settlement services, tax return preparation, and tax planning, is subject to the Act’s privacy notice.
* **Federal Trade Commission Act**: Key data security regulations governing law firms include the FTC Privacy Rule, FTC Safeguards Rule, and FTC Disposal Rule.
* **Fair and Accurate Credit Transactions Act**: Law firms subject to the FTC and GLB Acts must develop and implement a written identity theft prevention program.
* **State Laws**: Among other things, state laws require law firms to report data breaches to interested parties, and properly dispose of sensitive customer information when no longer needed.

**Professional Standards**:

Competent representation and confidentiality are at the foundation of the attorney-client relationship.

* **ABA Model Rule 1.1**, which covers the general duty of competent representation, provides: “Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”
	+ **Comment 8** notes that lawyers “should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.”
* **ABA Model Rule 1.6**, which covers the duty of confidentiality, provides: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” It is now commonly accepted in the legal profession that this duty applies to client information in computer and information systems.
	+ **Comment 18** notes that lawyers are required “to **act competently to safeguard information relating to the representation of a client** against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.”

The ABA Model Rules observe the existence of relevant state and federal privacy and data security laws that apply to attorneys and law firms, but note that the relevance of these laws is “beyond the scope of [the] Rules.” See **ABA Model Rule 1.6**, **Comments 18 and 19**.