The Gramm-Leach-Bliley Act of 1999 (GLB Act) includes provisions that are designed to protect consumers' personal financial information held by financial institutions.

The GLB Act gives eight federal agencies and the states the authority to administer and enforce the Financial Privacy Rule and the Safeguards Rule.

**Opt In / Opt Out**

**Opt Out – Federal Trend**

- **Definition.** GLB Act prohibits a financial institution, either directly or through an affiliate, from disclosing Non-public Personal Information ("NPI") to a nonaffiliated third party if the customer has not exercised his/her right to opt out.

- **SEC Regulated Organizations.** SEC Regulation S-P\(^1\) establishes the requirements for collecting and processing customer NPI. (Customers are persons).

- Under the GLB Act, consumers and customers have a right to opt out of having their information shared with third parties.

- The privacy notice must explain and must offer a reasonable way for a customer or consumer to do so.

- **Reasonable:** A firm can provide a toll free number or a detachable form with a pre-printed address so that customers can easily opt out.

- **Not reasonable:** Requiring someone to write a letter as the only way to opt out.

- **Exceptions:** The GLB Act does not give consumers the right to opt out when the financial institution shares information with its affiliates. While the GLB Act does not give people this right, a different law does: the Federal Credit Reporting Act.

- Under the FCRA, a consumer has the right to say no to the sharing of information, such as a credit report or application information, with the financial institution's affiliates.

- The privacy notice must make clear that a customer has the right to say no to the sharing of certain information with affiliated third parties.

- An affiliate is an entity that controls another company, is controlled by the company, or is

---

\(^1\) Regulations S-P (Privacy of Consumer Financial Information), 17CFR Part 248, SEC Release Nos. 34-42974, IC-24543, IA-1883; Amended in Release No. 34,50781 (effective January 11, 2005) to require procedures for proper disposal of consumer report information. Reg S-P applies to individual person, not entities. Hedge funds, for example, are not covered by Regulation S-P. See Staff Responses to Questions about Regulation S-P. See website at http://www.sec.gov/divisions/investment/guidance/regs2qa.htm.
under common control with the company.

♦ **No right to opt out:**
  - An individual **cannot** opt out if:
    - A financial institution shares information with outside companies that provide essential services like data processing or servicing accounts;
    - The disclosure is legally required;
    - A financial institution shares customer data with outside service providers that market the financial company's products or services.

♦ **Regulation S-P:**
  - **Regulation S-P Requires:**
    - Initial Privacy Notice
    - Annual Privacy Notice
  - **Specific Information to be Included in the Notice:**
    - Categories of NPI collected
    - Categories of NPI which might be disclosed
    - Categories of affiliate and non-affiliates to who NPI may be disclosed
    - Categories of NPI about former customers disclosed to affiliates and non-affiliates
    - Explanation of customer's opt-out right and how to exercise that right at any time
    - Policies and procedures to protect confidentiality and security
  - **Exceptions**
    - A firm may disclose consumer NPI only in the following circumstances:
      - The consumer consents;
      - To protect the confidentiality or security of the firm's records related to the consumer; protect against fraud; conduct institutional risk control; resolve customer disputes or inquires; communicate with a person holding a legal or beneficial interest related to the customer; or communicate with the customer's fiduciary
representative;

- Provide information to credit rating agencies, the customer's attorneys, accountants or auditors;
- As specifically allowed by law (e.g., law enforcement agencies, state regulatory agencies)
- Provide information to consumer rating agencies;
- The sale, merger or transfer of the business;
- To comply with federal, state or local laws.
- **Under the proposed rule:** A firm would be able to disclose consumer NPI when a departing RR/IAR joins another firm.

♦ **State Requirements:**
  
  o Federal law and rules do not pre-empt state laws.
  
  o States can provide greater protection than that afforded under federal law.
  
  o For example, states can specify the text size of the notice.

**Opt In – Some States and International Trend**

♦ Opt-In permits use of Personally Identifiable Information (PII) within the organization but "unambiguous consent" by customer is required before any such information can be shared with a non-affiliated third party.

♦ The Opt-In standard is most clearly enunciated by the European Union. The **European Data Protection Directive 95/46** requires satisfaction of several explicit requirements:
  
  o **Notice:** Must inform customer of:
    ▪ identity of information collector;
    ▪ uses for which information is collected
    ▪ how customer may control use of information
    ▪ where and to whom information may be transferred
    ▪ how customer can access their information

---


Standards: The ability to transmit customer data cross-borders requires compliance with extensive standards³

- Consent
- Consistency
- Access
- Security
- Onward transfer

- Some states do have an opt-in requirement, however, it depends both on the industry and the method for sharing information. For example: Connecticut and Illinois have opt-in for banking.

  - Some opt in states:
    - Alaska
    - California

  - E.g. Financial Information Privacy Act - Financial Code sections 4050 - 4060. This law prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer's consent, as provided. It provides for a plain-language notice of the privacy rights it confers. The law requires that (1) a consumer must "opt in" before a financial institution may share personal information with an unaffiliated third party, (2) consumers be given an opportunity to "opt out" of sharing with a financial institution's financial marketing partners, and (3) consumers be given the opportunity to "opt out" of sharing with a financial institution's affiliates, with some exceptions. When an affiliate is wholly owned, in the same line of business, subject to the same functional regulator and operates under the same brand name, an institution may share its customers' personal information with the affiliate without providing an opt-out right. [http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=04001-05000&file=4050-4060](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=04001-05000&file=4050-4060)

• Maine

• Massachusetts
  o *E.g.*: An “opt-in” requires the investment adviser to obtain from its customers and consumers a signed statement in which the person makes an affirmative declaration of permission to disclose such information. M.G.L. 110A.
  o See [http://www.sec.state.ma.us/sct/sctgbla/gblaidx.htm](http://www.sec.state.ma.us/sct/sctgbla/gblaidx.htm)

• North Dakota

• Vermont
  o *See* example of opt-in form.

• New Mexico

• Minnesota:
  o Has been interpreted as an opt-in state, however different companies have gotten different interpretations.