

# CRS Report for Congress

Received through the CRS Web

## Comparison of California's Financial Information Privacy Act of 2003 with Federal Privacy Provisions

M. Maureen Murphy  
Legislative Attorney  
American Law Division

### Summary

The California Financial Information Privacy Act,<sup>1</sup> enacted on August 28, 2003, and effective on July 1, 2004, governs the rights of California residents with respect to the dissemination of nonpublic personal information by financial institutions. In some respects, it diverges from two federal laws that impose restrictions on the dissemination of nonpublic personally identifiable customer information by financial information. Its major provisions include a requirement that before sharing nonpublic personal information with nonaffiliated third parties, financial institutions receive an affirmative consent, an opt-in, from their customers. Before such information may be shared with affiliates not in the same line of business and regulated by the same functional regulator, an opt-out notice is required. Wholly-owned subsidiaries and affiliates in the same line of business (securities, banking, or insurance) may share information, except medical information, without an opt-out or opt-in requirement. California's law was enacted just before Congress enacted the Fair and Accurate Credit Transactions Act (P.L. 108-159), which makes permanent federal statutory preemption of state regulation of information sharing among corporate affiliates that was set to expire on December 31, 2003, and limits the ability of affiliated companies to share consumer information for marketing solicitations. See CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law*; CRS Report RL32121, *Fair Credit Reporting Act: A Comparison of House and Senate Legislation*; CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law*, CRS Report RL31758, *Financial Privacy: The Economics of Opt-In vs Opt-Out*; and CRS Report RL31847, *The Role of Information in Lending: The Cost of Privacy Restrictions*. This report will be updated as warranted.

<sup>1</sup> 2003 Cal. Adv. Legis. Serv. 241 (West); 2003 Cal. Stat. Ch. 241. (Available September 3, 2003, in LEXIS, STATES Library, CACODE file.)

**Background.** There are two sets of federal rules for sharing of non-public personal information by financial institutions. One, under the Gramm-Leach-Bliley Act (GLBA), P.L. 106-102, applies to information sharing with non-affiliated third parties. The other, under the Fair Credit Reporting Act, specifically, the Fair Credit Reporting Act Amendments of 1996, P.L. 104-208, applies to information sharing among companies of the same corporate family or holding company, i.e., affiliates. GLBA prohibits financial institutions from sharing nonpublic personally identifiable customer information with non-affiliated third parties unless consumers are given an opportunity to prevent the disclosure, that is to opt out. Under its 1996 amendments, the Fair Credit Reporting Act (FCRA) preempts all state laws with respect to the exchange of information among affiliated entities, companies in the same corporate family. 15 U.S.C. § 1681t(b)(2). As amended in 2003, section 214 of P.L. 108-159, 117 Stat. 1952, the Fair and Accurate Credit Transactions Act of 2003, these preemptive provisions, due to expire at the end of 2003, were made permanent. An additional limitation was placed on information sharing among affiliated companies. Subject to certain exceptions, affiliated companies may not share customer information for marketing solicitations unless the consumer is provided clear and conspicuous notification that the information may be exchanged for such purposes and an opportunity and a simple method to opt-out.

The California Financial Information Privacy Act was enacted as the 1996 FCRA temporary preemption of state law was about to expire and contemporaneously with Congressional consideration of proposals to extend the FCRA preemption. Its provisions respecting information sharing among corporate affiliates are subject to the preemption provisions of the FCRA. Any provisions of the California law that relate to information sharing by financial institutions with non-affiliated third parties and that provide more protection than GLBA's privacy provisions would not be preempted.

**Current Legislation.** Among the bills being considered by the 108<sup>th</sup> Congress are the following:

H.R. 2622 (Representative Bachus), which has been reported by the House Financial Services Committee (H.Rept. 108-263) and passed by the House, would, among other things, make permanent the FCRA preemptions respecting information sharing among affiliates.

H.R. 1766 (Representative Tiberi and Lucas), in addition to making the FCRA preemptions permanent, would give preemptive effect to GLBA's provisions respecting disclosure of nonpublic personal information by financial institutions, effectively establishing a national standard for disclosure of customer information by financial institutions. It would prevent states and local governments from imposing additional requirements, such as an opt-in for information sharing with non-affiliated third parties, more detailed or more frequent notice requirements, or increased protection for sensitive data.

S. 660 (Sen. Johnson) would make the FCRA preemptions permanent, thereby preempting state laws or regulations restricting information sharing among corporate affiliates.

**California Financial Information Privacy Act.** The following comparison with existing federal law is presented as a means of focusing on some of the issues that Congress has been examining.

*California Law*

*Federal Law*

*Nonaffiliated 3d Parties*

|   |                 |
|---|-----------------|
| <p>Opt-in for a financial institution to share non-public personal information (NPPI) with nonaffiliated third parties.</p> | <p>Opt-out.</p> |
|---|-----------------|

*“Affiliates”*

|   |   |
|---|---|
| <p>Entities controlled by or under common control with another entity. Has separate rules for wholly-owned financial affiliates that are in the same line of business (banking or insurance or securities), regulated by the same functional regulator, and use the same brand. (Hereafter, wholly-owned affiliates.)</p> | <p>Same definition. Has no distinction for “wholly-owned affiliates.”</p> |
|---|---|

*Information Sharing Among Affiliates*

|   |   |
|---|---|
| <p>No opt-out or opt-in requirement for sharing of NPPI among wholly-owned financial affiliates. Medical information is excluded and may be shared only pursuant to another Cal. statute.</p> | <p>Permits all affiliates to share experience and transaction information without an opt-in or an opt-out.</p>              |
| <p>Opt-out for financial institution to share NPPI information with affiliates other than those meeting the criteria for “wholly-owned financial affiliates.”</p>                             | <p>Opt-out required for financial institutions to share non-experience or non-transaction information among affiliates.</p> |
|   | <p>No distinction for medical information.</p>  |

*“Financial Institution”*

|   |                            |
|---|----------------------------|
| <p>Excludes computer services, lawyers (and possibly, accountants), and motor vehicle dealers assigning sales contracts to financial institutions in 30 days.</p> | <p>No such exclusions.</p> |
|---|----------------------------|

*“Consumer” or “Customer”*

|   |                            |
|---|----------------------------|
| <p>Excludes beneficiaries of employee benefit plan, group insurance plan, worker compensation plan, or trust.</p> | <p>No such exclusions.</p> |
|---|----------------------------|

*Consent Form for Opting In*

|   |                        |
|---|------------------------|
| <p>There must be: clear notice that it remains in effect until revoked; of procedures for revocation; and, that a copy may be requested. Signature required. Institution may not discriminate because consent has been withheld, but may offer incentive to obtain consent.</p> | <p>Not applicable.</p> |
|---|------------------------|

*Opt-Out Requirements*

|  |   |
|--|---|
| <p>Must provide an annual written notice to the consumer that the financial institution may disclose NPPI to affiliates and that the consumer has not yet opted out.</p> <p>If a common data base is maintained with affiliates, once the consumer has opted out, NPPI in that data base may not be further disclosed or used by an affiliate except as permitted.</p> | <p>One time notice sufficient. No details of content and form specified by statute; nor are there statutory requirements for self-addressed return envelopes, model notice and consent forms, or a means of regulatory approval of forms. The regulations provide more detail than the statute as to content and form for consent but are not as specific as is the California law.</p> |
|--|---|

Statute contains detailed specifications regarding form and content of opt-out notice, including requirements for providing return envelopes and, in some instances, postage paid return envelopes. Statute provides a model form that acts as presumptive proof of compliance if used to notify of opt-out right. An alternative permits financial institutions to submit forms for approval by functional regulators.

*Joint Marketing Agreements*

|   |   |
|---|---|
| <p>Opt-out is required for joint marketing agreements entered into after January 1, 2005 if certain conditions are met; otherwise opt-in is required. Conditions require that the product or service be that of one of the parties, jointly offered with notice of the financial institutions that have the NPPI, and the agreement must provide for confidentiality.</p> | <p>No opt-out requirement for joint marketing agreements if the customer has notice that the information will be provided and the receiving institution agrees to maintain its confidentiality. No further limitations on the services offered or notices to be provided with those marketing offers.</p> |
|---|---|

*Account Number*

|                       |  |
|-----------------------|--|
| No specific provision | Account numbers may not be disclosed for marketing to nonaffiliated third parties. |
|-----------------------|--|

*Annual Notice of Privacy Policy*

|  |   |
|--|---|
| No requirement for annual notice of privacy policy other than annual notice that the institution may disclose NPPI to affiliates and the customer has not opted out. | GLBA requires initial and annual notice of financial institution's privacy policy and specifies information to be included. |
|--|---|

*Affinity Partnerships*

|  |   |
|--|---|
| Requires a written confidentiality agreement. Limits information financial institutions may provide to an affinity partner with whom it issues a credit card or provides services, primarily to name, address, and record of purchases with affinity card. | GLBA has no explicit provision for affinity agreements. |
|--|---|

*Exceptions*

|   |                                      |
|---|--------------------------------------|
| Similar to those in GLBA. Explicitly includes USA PATRIOT Act requirements, and various provisions permitting reporting suspected illegal activity, such as elder abuse or identity theft, and administering various programs—such as collection of child support, bone marrow donations. | Has an extensive list of exceptions. |
|---|--------------------------------------|

*Enforcement*

|  |   |
|--|---|
| Prescribes liability of up to \$2,500 per consumer for each violation, up to \$500,000, enforceable by the California Attorney General and the California and federal functional regulators. | Administrative enforcement by functional regulators—federal banking and securities regulators; state insurance regulators, and FTC for entities not subject to other regulator. |
|--|---|