Study B-400 May 7, 2003

Memorandum 2003-19

Financial Privacy (Discussion of Issues)

The Commission initiated consideration of the financial privacy study at its February 2003 meeting, with an overview of the area. At that meeting the Commission made several initial policy decisions and identified matters for further research. This memorandum seeks to advance the process by presenting statute drafts for those policy matters that were decided and by presenting discussion of those matters for which further research was called.

The following material is attached to this memorandum and discussed at appropriate points in the memorandum:

In addition, a number of key documents are attached to the overview memorandum considered at the February meeting — Memorandum 2003-1. The attachments to that memorandum include copies of ACR 125 (Papan), the Title V of the Financial Services Modernization Act (commonly known as the Gramm-Leach-Bliley Act or GLB), and SB 1 (Speier).

To facilitate navigation in this lengthy memorandum, we set out below an outline of the memorandum. In the text of the memorandum we highlight staff recommendations in boldface.

OUTLINE OF MEMORANDUM

COMMISSION'S MANDATE

The Law Revision Commission's mandate for this study is found in ACR 125 (Papan), enacted as 2002 Cal. Stat. res. ch. 167. The resolution directs the Commission to study, report on, and prepare recommended legislation by January 1, 2005, concerning the protection of personal information relating to, or arising out of, financial transactions. The resolution specifies that the proposed legislation should accomplish the following objectives:

(1) Provide consumers with notice and the opportunity to protect and control the dissemination of their personal information.

(2) Direct the preparation of regulations that recognize the inviolability and confidentiality of a consumer's personal information and the

legitimate needs of entities that lawfully use the information to engage in commerce.

(3) Assure that regulated entities will be treated in a manner so that, regardless of size, an individual business, holding company, or affiliate will not enjoy any greater advantage or suffer any burden that is greater than any other regulated entity.

(4) Be compatible with, and withstand any preemption by, the Gramm-Leach-Bliley Act and the federal Fair Credit Reporting Act.

(5) Provide for civil remedies and administrative and civil penalties for a violation of the recommended legislation.

2002 Cal. Stat. res. ch. 167.

The impetus for this study is laid out in the resolution. GLB liberalizes the ways that financial institutions may share nonpublic personal information, thereby illuminating the extent to which financial institutions buy, sell, and use that information. GLB does not, however, provide a comprehensive framework by which individuals may control this activity. Instead, it grants individuals limited control over sharing of their personal information by financial institutions, and leaves it to the states to provide for greater privacy protection.

The Commission has recognized that there is substantial other legislative activity in progress on the matter, both in the California Legislature and in Congress, as well as a potential ballot initiative. Moreover, it is likely that significant action in one or more of these venues will occur before completion of the Commission's study. In that case, the character of the Commission's final recommendation would necessarily be fundamentally affected.

The Commission has decided to proceed, for now, as if no other definitive legislative action will occur before completion of this study. But the Commission is prepared to shift focus and concentrate instead on problems in or potential improvements of any legislation that is enacted before completion of the study.

CURRENT DEVELOPMENTS

This portion of the memorandum summarizes current developments that affect this project. If we become aware of any significant developments between the date of issuance of the memorandum and the meeting at which it is considered, we will update the memorandum either by a supplemental memorandum or orally at the meeting.

State Activities

California Legislature

SB 1 (Speier), proposing the California Financial Information Privacy Act, has passed the Senate. The bill is double-referred in the Assembly to the Banking and Finance Committee and the Judiciary Committee. It is currently set for hearing in the Banking and Finance Committee on May 12.

Local Public Entities

Local ordinances purporting to regulate information practices of banks within their jurisdictions have been challenged by banks in the federal district court for Northern California. The initial complaint was filed in September 2002 and a summary judgment motion by the plaintiffs was filed in October 2002. That motion is pending. Depositions have been taken. Meanwhile, the court has made a related case order for the two cases of *Bank of America, Wells Fargo, et al. v. Daly City*, No. 02-4343 (N.D. Cal.) (seeking declaratory and injunctive relief on federal preemption and constitutional grounds) and *Bank of America, Wells Fargo, et al. v. Contra Costa*, No. 02-4943 (N.D. Cal.).

A comparable ordinance has now been proposed for adoption by the Marin County Board of Supervisors. It would apply to unincorporated areas of the county. It is scheduled for vote on May 13. Similar ordinances have been adopted by Alameda, Contra Costa, San Francisco, San Mateo, and Santa Clara counties, as well as by Daly City.

Ballot Initiative

A proposed ballot initiative — the "California Financial Privacy Act" — has cleared the Secretary of State and Attorney General for petition circulation. The proponents have until September 29 to gather the necessary signatures. Due to the low turnout at the last gubernatorial election, only 373,816 valid signatures are required.

The Attorney General's title and summary of the chief purpose and points of the proposed measure states:

> **Consumer Information Privacy. Initiative Statute.**
> Prohibits entities engaged in consumer financial-related activities defined in federal law, from disclosing information about a California consumer without the consumer's informed consent. Financial-related activities include: lending; transferring; investing for others, or safeguarding money or securities; insuring;

underwriting; providing financial or investment advice. Prohibition covers disclosure to business affiliates and third parties. Exceptions include: processing transactions requested by consumer, detecting and preventing fraud and enforcing laws. Doubles civil penalties for violations that result in use of information by a person to falsely obtain credit, goods, services or medical information in another's name.

Summary of estimate by Legislative Analyst and Director of Finance of fiscal impact on state and local governments: This measure would result in state and local government enforcement costs potentially over $1 million annually, partially offset by increased civil penalty revenues. Depending on implementation issues, the measure could also result in some state and local compliance costs and some revenue reductions.

A copy of the measure is attached at Exhibit p. 20.

Financial Services Privacy Coalition

The Financial Services Privacy Coalition is an alliance of the California Chamber of Commerce, the California Bankers Association, the American Insurance Association, the Securities Industry Association. the Personal Insurance Federation of California, and the Association of California Life and Health Insurance Companies. The coalition is opposed to enactment of SB 1 (Speier) for a number of reasons. See Exhibit p. 17.

The coalition is supposed to have issued a position paper that sets out the approach to financial privacy protection that it advocates. However, the staff has been unable to obtain a copy of that paper. To the extent we can glean their position on various issues from their opposition letter to SB 1, we do so in this memorandum.

Law Revision Commission Study

Our study of this matter is due by January 1, 1995. There are a number of obstacles confronting us, such as the statewide hiring and contract freeze (hindering the Legislature's intention to make it possible for the Commission to complete this project without impairing progress on other studies) and the directive to state advisory bodies to restrict their meeting schedules.

The major problem, however, is that the tenor of the Commission's final recommendation is totally dependent on actions in Congress, in the California Legislature, and in the ballot initiative process. For now, we can only proceed on

the assumption that nothing will occur in those venues before January 1, 1995, and be prepared to shift focus if there is a change in circumstances.

Federal Activities

Gramm-Leach-Bliley Act

We have understood that an effort would be made in Congress this year to forge a compromise that would amend the Gramm-Leach-Bliley Act to provide greater privacy protection, in exchange for state preemption. The staff is monitoring developments in Congress. Obviously, a federal decision reversing the preemption situation would go to the heart of the current study.

One piece of federal legislation would amend GLB to provide greater privacy protection, but whether it would also preempt state financial privacy laws is unclear. The measure as introduced does not directly repeal the provision of GLB that allows for more protective state laws on financial privacy. See discussion of the "Privacy Act of 2003" below.

Another piece of federal legislation would amend GLB to preempt any state law on the subject without enacting greater privacy protection:

> **Relation to State Laws**
>
> No requirement or prohibition may be imposed under the law of any State, or any political subdivision of any State, with respect to any subject matter regulated under or addressed by any provision of this subtitle.

H.R. 1766 (Tiberi), introduced April 11, 2003, to enact the "National Uniform Privacy Standards Act of 2003".

A third measure would enact comprehensive privacy legislation but preserve the effect of GLB. The measure would appear to preempt state financial privacy legislation. See discussion of the "Consumer Privacy Protection Act of 2003" below.

Meanwhile, Illinois and Vermont have preemption determinations pending before the Federal Trade Commission (FTC). (North Dakota and Connecticut have previously received FTC determinations that their financial privacy statutes are not preempted by GLB).

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) preempts, until January 1, 2004, state statutes governing exchange of information among affiliates, and various other provisions of FCRA. After that date a state may enact a statute addressed to those

provisions, provided that the statute states explicitly that it is intended to supplement the FCRA and that it gives greater protection to consumers than is provided under FCRA. 15 U.S.C. § 1681t(d).

We have understood that an effort would be made in Congress this year to extend the January 1, 2004, date. Two recently introduced measures, rather than extending the preemption period, would make FCRA preemption permanent:

> *(d) Limitations.* Subsections (b) and (c)
> ~~(1)~~ do not affect any settlement, agreement, or consent judgment between any State Attorney General and any consumer reporting agency in effect on the date of enactment of the Consumer Credit Reporting Reform Act of 1996~~; and~~
> ~~(2) do not apply to any provision of State law (including any provision of a State constitution) that~~
> ~~(A) is enacted after January 1, 2004;~~
> ~~(B) states explicitly that the provision is intended to supplement this title; and~~
> ~~(C) gives greater protection to consumers than is provided under this title~~.

S. 660 (Johnson), introduced March 19, 2003, to enact the "Economic Opportunity Protection Act of 2003"; H.R. 1766 (Tiberi), introduced April 11, 2003, to enact the "National Uniform Privacy Standards Act of 2003".

SJR 2 (Figueroa) highlights the January 1, 2004, issue and memorializes Congress not to preempt state privacy laws:

> WHEREAS, We note that this opportunity may soon avail itself, as the Fair Credit Reporting Act, 15 U.S.C. Sec. 1681 et seq., prevents states from imposing any requirement or prohibition with respect to certain provisions of that act, unless that requirement or prohibition gives greater protection to consumers and is enacted after January 1, 2004; now, therefore, be it
> *Resolved by the Senate and Assembly of the State of California, jointly,* That the Legislature of the State of California respectfully requests that the Congress of the United States exempt from preemption any state privacy law that provides greater protection to consumers than is, or will be, provided by federal law.

The measure is pending in Senate Judiciary Committee.

Privacy Act of 2003

Senator Feinstein has introduced in Congress S. 745 (March 31, 2003), which would enact the "Privacy Act of 2003". The measure would broadly prohibit a

commercial entity from collecting personally identifiable information and disclosing it to a nonaffiliated third party for marketing purposes or selling it to a nonaffiliated third party unless the commercial entity first discloses its intention and provides an individual an opportunity to opt out.

The measure is not intended to affect the applicability or enforceability of GLB, but it would amend GLB significantly — along the lines of SB 1 (Speier) — so that:

(1) *Affiliates.* A consumer would have the right to opt out of information sharing by a financial institution with its affiliates. (Under GLB, there is no opt out right for affiliate sharing.) However, a financial institution could provide information to an affiliate that performs services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, free of the opt out right.

(2) *Nonaffiliated third parties.* A financial institution could not share personal information with a nonaffiliated third party unless the consumer opts in. (Under GLB, a consumer may opt out of nonaffiliated third party information sharing.) Again, a financial institution could provide information to a nonaffiliated third party that performs services for or functions on behalf of the financial institution, even though the consumer has not opted in.

(3) *Joint marketing agreements.* A consumer would have a right to opt out of information sharing with nonaffiliated third parties with which the financial institution has a joint marketing agreement. (Under GLB, there is no opt out right for joint marketing agreement sharing.)

(4) *Denial of service.* The measure would prohibit a financial institution from denying service to a consumer as a result of the consumer's refusal to grant consent to disclosure.

While S. 745 would preserve the operation of GLB as amended, it is not clear whether the measure is intended to preempt state law that goes beyond GLB. Title I of the bill, relating to commercial sale and marketing of personally identifiable information generally, is intended to preempt state law. It states, "The provisions of this title shall supersede any statutory and common law of States and their political subdivisions insofar as that law may now or hereafter relate to the -- (1) collection and disclosure of personally identifiable information for marketing purposes; and (2) collection and sale of personally identifiable information." Sec. 105.

This would be broad enough by its terms to preempt state financial privacy laws. However, Title I also states that, "Nothing in this title is intended to affect the applicability or the enforceability of any provision of, or any amendment made by ... title V of the Gramm-Leach-Bliley Act." Sec. 102(e)(3)(B). This presumably would preserve as law the provisions of GLB that permit more protective state financial privacy laws. And in fact, S. 745 makes a number of amendments to GLB, but it does not touch the GLB provisions on preemption.

The staff believes a strong argument could be made either way on whether S. 745 would preempt state financial privacy laws, at least with respect to disclosure of personally identifiable information for marketing purposes or sale. (Note. Similar arguments can be made with respect to the Fair Credit Reporting Act preemption rules. FCRA is likewise unaffected by the measure. Sec. 102(e)(3)(D).)

Consumer Privacy Protection Act of 2003

Representative Stearns has introduced the "Consumer Privacy Protection Act of 2003" (April 3, 2003). This measure has attracted attention because Representative Stearns is Chairman of the House Subcommittee on Commerce, Trade, and Consumer Protection, and the measure is sponsored by a bipartisan group, many of whom are members of that committee.

Key feature of the measure include:

(1) It covers all entities that collect, sell, disclose for consideration, or use personally identifiable information of a consumer.

(2) It excludes from its coverage government agencies, nonprofit organizations, certain small businesses, and professionals subject to client confidentiality requirements.

(3) It requires a privacy notice to a consumer in the first instance, but does not require a privacy notice annually thereafter.

(4) A consumer would have an opt out opportunity. The opt out would last for five years.

(5) It would allow self-regulatory control of compliance on approval of the program by FTC.

(6) With respect to financial privacy, the measure would defer to and be superseded by GLB and FCRA.

(7) The measure would preempt all state legislation in the area:

> This title preempts any statutory law, common law, rule, or regulation of a State, or a political subdivision of a State, to the extent such law, rule, or regulation relates to or affects the collection, use, sale, disclosure, retention, or dissemination of personally identifiable information in commerce. No State, or political subdivision of a State, may take any action to enforce this title.

As with S. 745 (Feinstein), there is some ambiguity about the intention of this bill on financial privacy preemption. Unlike S. 745, however, this bill defers to GLB in such a way that it does not appear to accept GLB's weak preemption provision. (The bill does not affect the operation of GLB "with respect to Federal rights and practices.") Moreover, although the bill does not repeal GLB's preemption provision, neither does it directly amend any of GLB's other provisions. The staff believes that despite some ambiguity, the measure as currently drafted would be construed to preempt state financial privacy laws.

Empirical Study

GLB requires the Secretary of the Treasury, in conjunction with the Federal Trade Commission and other federal regulators, to make a study and report to Congress with findings and conclusions on the following matters:

- The purposes for the sharing of confidential customer information with affiliates or with nonaffiliated third parties.
- The extent and adequacy of security protections for such information.
- The potential risks for customer privacy of such sharing of information.
- The potential benefits for financial institutions and affiliates of such sharing of information.
- The potential benefits for customers of such sharing of information.
- The adequacy of existing laws to protect customer privacy.
- The adequacy of financial institution privacy policy and privacy rights disclosure under existing law.
- The feasibility of different approaches, including opt out and opt in, to permit customers to direct that confidential information not be shared with affiliates and nonaffiliated third parties.
- The feasibility of restricting sharing of information for specific uses or of permitting customers to direct the uses for which information may be shared.

15 USC § 6808(a). The study was due on or before January 1, 2002.

The study and report are in progress and according to the Treasury Department will be released soon. The report will compile the responses of interested parties to the questions posed by GLB, and therefore will be qualitative rather than quantitative in character. We will obtain the report when it becomes available. The report should prove helpful to the Commission in formulating policy decisions.

STATE REGULATORY AUTHORITY

Function of State Regulatory Authority

The staff proposes to resolve a number of the issues raised in this memorandum through involvement of a state regulatory authority. A state regulator can, for example:

- Be of assistance in prescribing the specific application of a general statutory standard.
- Keep state law in conformity with (and free of preemption by) federal law as federal regulations change, by adopting conforming state regulations.
- Promulgate standard forms that may be more user friendly than a statutory form and may be more readily adjusted for changes in state law.
- Play a useful role in enforcement of the law.

The enabling resolution for this study contemplates a significant role for the state regulatory authority. The resolution includes a direction that the recommended legislation, "Authorize and direct affected regulators to prepare regulations that will recognize the inviolability and confidentiality of a consumer's personal information and the legitimate needs of entities that lawfully use the information to engage in commerce at the behest of consumers or for their benefit." The enabling resolution also directs that the recommended legislation provide for administrative penalties for a violation of the recommended legislation. 2002 Cal. Stat. res. ch. 167.

The primary concern of the staff with this approach is one of cost. With the state budget in crisis, the prospect of trying to establish a new state regulatory regime is daunting. On the other hand, with a due date for the Commission's recommendation of January 1, 2005, and a prospective operative date of implementing legislation of January 1, 2006, or later, the situation may well have stabilized by then.

Which Agency?

One question is which agency should be the state regulatory authority? Because the scope of the privacy statute is so broad — applicable to banks, insurance companies, securities dealers, and many other businesses and professions that are substantially involved in "financial" activities — any of a number of state regulators could arguably play a role. In fact, under GLB, regulatory authority is allocated among seven different federal agencies, plus state insurance commissioners. 15 USC §§ 6804, 6805.

The staff does not think division of authority is a good idea here. GLB seeks to avoid undue complexity by directing the various federal agencies to "consult and coordinate" with each other so that, to the extent possible, the various regulatory regimes are compatible with each other. 15 USC § 6804(a)(2). And in fact, this has been done, with all federal regulations being generally consistent with the regulations adopted by the Federal Trade Commission (the lead agency under GLB). See 16 CFR Part 313, attached as Exhibit p. 1.

But the complexity inherent in allocation of regulatory authority among a number of different regulators will be aggravated by further fragmentation at the state level. The staff thinks we need to keep things as simple and clear as possible. That translates to a single state regulatory authority.

The staff thinks **we should consider the state Office of Privacy Protection** (OPP) as the state regulatory authority. The mandate of that office is to protect the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices. Bus. & Prof. Code § 350. OPP began operation in 2001; it is in the Department of Consumer Affairs. OPP is not new to financial privacy issues, and already devotes a section of its informative website to the matter. See www.privacy.ca.gov.

This role would be a significant expansion of OPP's jurisdiction. But the Department of Consumer Affairs certainly has regulatory experience of this nature. An added benefit is that OPP could not be considered "captive" of any of the industries that would be subject to its regulatory authority under the statute.

The staff has floated this suggestion to OPP for its reaction. OPP is currently reviewing the suggestion.

In any event, this memorandum uses the term *state regulatory authority* in the various proposed statute drafts. After we have decided which agency is most

appropriate, we would replace references to the state regulatory authority with references to the identified agency.

Draft Statute

Regardless of which agency is selected as the state regulatory authority for financial privacy purposes, the statute might look something like this:

> **State regulatory authority**
>
> (a) Regulatory authority under this chapter is vested in the *state regulatory authority*.
>
> (b) Rulemaking authority under this chapter is subject to the administrative regulations and rulemaking provisions of the Administrative Procedure Act, Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code.
>
> (c) Administrative adjudication authority under this chapter is subject to the administrative adjudication provisions of the Administrative Procedure Act, Chapters 4.5 (commencing with Section 11400) and 5 (commenting with Section 11500) of Part 1 of Division 3 of Title 2 of the Government Code. An administrative hearing under this chapter shall be conducted by an administrative law judge assigned by the Office of Administrative Hearings pursuant to Chapter 4 (commencing with Section 11370) of Part 1 of Division 3 of Title 2 of the Government Code.
>
> (d) The sum of $185,000 dollars is appropriated from the General Fund to the *state regulatory authority* for the 2005-06 fiscal year for purposes of this chapter.
>
> **Comment.** Functions of the *state regulatory authority* under this chapter include adoption of regulations that define the scope of the chapter and the meaning of critical terms used in the chapter, determination of specified exemptions from application of the chapter, promulgation of the form of privacy notices required by this chapter, enforcement of duties under the chapter, and maintenance of conformity of the chapter with, and exemption from preemption by, federal laws. See Sections [*to be provided*].

The amount appropriated assumes two attorneys, two analysts, and one secretary, based on half year funding, assuming a January 1, 2006, operative date. The initial effort would be adoption of regulations. That would later shift to enforcement. Response to inquiries would be a major function throughout.

Note that an appropriation requires a two-thirds vote. Whether this will be achievable, given the political dynamics at work here, is speculative.

General Discussion

The enabling resolution for this study requires the Commission to prepare recommended legislation concerning the protection of personal information relating to, or arising out of, financial transactions. The resolution does not define those terms.

One of the objectives of the recommended legislation is to be compatible with, and withstand preemption by, the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. The Commission has decided that, at least initially, it would conform the scope of this study to the information and transactions that are subject to those acts. The Commission requested further information about the scope of those statutes, and whether there might be a general standard that could be used to distinguish "financial" from other commercial transactions.

GLB regulates disclosure by a financial institution of nonpublic personal information. GLB's control of information sharing is status-based rather than transactional. It focuses on the entities involved and their relationships to each other rather than the purposes for which the information is shared among the entities.

FCRA regulates consumer reports — the communication of credit information about a consumer. (That may include information that bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.) FCRA thus controls a narrow segment of the universe governed by GLB, and GLB expressly defers to FCRA in that area. FCRA limits the purposes for which credit information may be shared and the uses to which it may be put. FCRA's regulatory approach is transactional rather than status based.

Financial Institution

GLB governs the activities of financial institutions. Under GLB, a financial institution is any business institution that is significantly engaged in "financial activities" as described in the Bank Holding Company Act, 12 USC § 1843(k). See 15 USC § 6809. That would include activities of credit bureaus to the extent not governed by FCRA. (GLB provides a few exceptions to the general rule, exempting an entity within the jurisdiction of the Commodity Futures Trading Commission, the Federal Agricultural Mortgage Corporation, or chartered by

Congress specifically to engage in a proposed securitization, secondary market sale, or similar transaction). 15 USC § 6809(3) ("financial institution" defined).

In turn, financial activities within the meaning of the Bank Holding Company Act include, among other matters:

> (A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities.
>
> (B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State.
>
> (C) Providing financial, investment, or economic advisory services, including advising an investment company (as defined in section 3 of the Investment Company Act of 1940.
>
> (D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.
>
> (E) Underwriting, dealing in, or making a market in securities.

12 USC § 1843(k)(4).

Implementing regulations of the Federal Trade Commission give a broad interpretation to the Bank Holding Company Act standard. Under the Final Rule promulgated by FTC, an institution must be significantly engaged in financial activities to be considered a financial institution for GLB purposes.

FTC considers the following activities to be financial:

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities; insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death; providing financial investment or economic advisory services; underwriting or dealing with securities.
- Engaging in an activity that the Federal Reserve Board has determined to be closely related to banking. For example:
  - Extending credit and servicing loans
  - Collection agency services
  - Real estate and personal property appraising
  - Check guaranty services
  - Credit bureau services
  - Real estate settlement services
  - Leasing real or personal property (on a nonoperating basis for an initial lease term of at least 90 days)
  - Engaging in an activity that a bank holding company may engage in outside of the United States. For example:
  - Operating a travel agency in connection with financial services

Examples of businesses that engage in these sorts of financial activities and are therefore financial institutions for purposes of GLB Act are:

- Mortgage lender or broker
- Check casher
- Pay-day lender
- Credit counseling service and other financial advisors
- Medical-services provider that establishes for a significant number of its patients long-term payment plans that involve interest charges
- Financial or investment advisory services including tax planning, tax preparation, and instruction on individual financial management
- Retailer that issues its own credit card
- Auto dealers that lease and/or finance
- Collection agency services
- Relocation service that assists individuals with financing for moving expenses and/or mortgages
- Sale of money orders, savings bonds, or traveler's checks
- Government entities that provide financial products such as student loans or mortgages

Note, however, that only institutions "significantly engaged" in financial activities are subject to GLB. Whether a financial institution is significantly engaged in financial activities is a flexible standard that takes into account all the facts and circumstances. Examples of businesses that are **not** significantly engaged for purposes of GLB are:

- Retailer that does not issue its own credit card (even if it accepts other credit cards)
- Grocery store that allows consumers to get cash back by writing a check in an amount higher than the actual purchase price
- Merchant who allows an individual to "run a tab"
- Retailer that provides occasional "lay-away" and deferred payment plans or accepting payment by means of credit cards issued by others as its only means of extending credit

How can we capture the broad and nebulous scope of federal law by state statute? The staff thinks it is futile to try by statute to describe the types of businesses that are considered to be "financial institutions" for purposes of GLB

privacy protections. Moreover, we cannot simply refer to the federal statute; we must also pick up federal regulations that temper the meaning of the statute.

Unfortunately, there are seven federal agencies, plus state insurance authorities, with regulatory responsibility under GLB. Fortunately, GLB requires each agency and authority to consult and coordinate "for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities." 15 USC § 6804(a)(2). This directive has been followed by the affected regulators.

An added problem with trying to capture the federal law in the California statute is that much of the federal law is found in regulations, and regulations may change more readily than the underlying statute. California's codification of a particular federal interpretation may become inconsistent with federal law (and perhaps cause federal preemption of California law) if the federal regulation is changed.

Would it help matters to have a state regulator acting as intermediary to provide guidance to businesses as federal regulations change and the meaning of state law changes with them? The staff thinks so.

While it may not be possible to capture the full meaning of federal law in a statute, there are two useful steps we can take. We can direct the California regulatory authority to promulgate regulations that conform to the federal law and regulations. And meanwhile we can reproduce some of the detail of existing federal law in the Comment. Law Revision Commission Comments are reproduced by law publishers in the annotated codes and therefore will be accessible to attorneys providing advice to businesses in this complex area.

The staff thinks **a provision along the following lines would be sufficient to pick up coverage of GLB** for purposes of California's privacy regulation:

> **Scope of Chapter**
>
> (a) This chapter applies to disclosure of nonpublic personal information by a business that is a "financial institution" within the meaning of the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6809(3), and implementing regulations adopted pursuant to 15 USC § 6804.
>
> (b) The *state regulatory authority* shall by regulation elaborate the application of this chapter.
>
> **Comment.** The intent of this section is that the coverage of California's financial privacy law be coextensive with the coverage of the Gramm-Leach-Bliley Act. Although the Gramm-Leach-Bliley

Act uses the term "financial institution", its application extends to other businesses besides traditional banking entities such as banks, savings and loan associations, and credit unions. A principle objective of the Gramm-Leach-Bliley Act (Financial Services Modernization Act) is to liberalize the types of business a financial entity may engage in, including banking, securities, and insurance.

Under federal law, 15 USC § 6809(3), a financial institution is a business that is engaged in financial activities as described in the Bank Holding Company Act, 12 USC § 1843(k). There are some exceptions to the general rule — an entity within the jurisdiction of the Commodity Futures Trading Commission, the Federal Agricultural Mortgage Corporation, or chartered by Congress specifically to engage in a proposed securitization, secondary market sale, or similar transaction is not a financial institution for purposes of the federal law.

Financial activities within the meaning of the Bank Holding Company Act, 12 USC § 1843(k)(4), include, among other matters:

(A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities.

(B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State.

(C) Providing financial, investment, or economic advisory services, including advising an investment company (as defined in section 3 of the Investment Company Act of 1940.

(D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.

(E) Underwriting, dealing in, or making a market in securities.

Implementing federal regulations give a broad interpretation to the Bank Holding Company Act standard. Under the Federal Trade Commission regulations, an institution must be significantly engaged in financial activities to be considered a financial institution for GLB purposes. 16 CFR 313.3(k)(1).

The federal regulations provide examples of activities that are considered financial. See 16 CFR. 313.3(k)(2)(i)-(xii) (Federal Trade Commission regulations); see also 12 CFR 716.3(*l*)(2) (National Credit Union Administration regulations).

Note, however, that only an institution significantly engaged in financial activities is subject to GLB, and this chapter. Whether a financial institution is significantly engaged in financial activities is a flexible standard that takes into account all the facts and circumstances. The federal regulations also provide examples of businesses that are not significantly engaged for purposes of GLB.

> See 16 CFR 313.3(k)(4)(i)-(iv) (Federal Trade Commission regulations).

Despite the broad application of GLB, it does not modify, limit, or supersede the operation of the Fair Credit Reporting Act. 15 USC § 6806. That law governs the exchange of personal financial information about an individual in a "consumer report" between a consumer reporting agency and a third party. 15 USC § 1681a. The purpose of FCRA is to require credit bureaus to adopt reasonable procedures for meeting the needs of commerce for credit information in a manner that is fair and equitable to the consumer with regard to the confidentiality, accuracy, relevancy, and proper use of credit information.

The preemption rules governing interaction of FCRA and state privacy legislation are complex. See discussion of "Federal Preemption" below. For this reason, the **staff proposes that we not attempt to draft scope legislation on FCRA at this time**, but to focus instead on GLB scope. Any necessary FCRA carve-outs can be done later.

Attorneys and Others in a Confidential Relationship

The very broad application given the term "financial institution" under federal law leads to some anomalous results. An attorney who is substantially engaged in a tax or estate planning practice, for example, has been determined by the FTC to be a financial institution for purposes of GLB, and subject to the privacy notice and other requirements of the federal law. However, state law generally imposes greater confidentiality requirements on attorney-client relationships than does federal financial privacy law.

The American Bar Association has filed suit in federal court to overturn the FTC determination. That lawsuit is pending. Nineteen state and local bar associations have filed an amicus brief in support of the ABA position.

A bill also has been introduced in Congress to exempt attorneys from GLB:

> Notwithstanding subparagraph (A), the term "financial institution" does not include attorneys at law who are subject to, and in compliance with, regulation of client confidentiality in the form of rules of professional conduct promulgated either by the court of highest appellate authority or by the principal legislative body of any State of the United States, the District of Columbia, any territory of the United States, Puerto Rico, Guam, American Samoa, the Trust Territory of the Pacific Islands, the Virgin Islands, or the Northern Mariana Islands.

H.R. 781 (Biggert), introduced February 13, 2003, as the "Privacy Protection Clarification Act". Congress has not yet acted on the measure.

A more comprehensive approach to this problem is suggested by SB 1 (Speier). That bill would exempt from state financial privacy laws a provider of professional services that is bound by overriding confidentiality requirements:

> The term "financial institution" does not include any provider of professional services, or any wholly owned affiliate thereof, that is prohibited by rules of professional ethics or applicable law from voluntarily disclosing confidential client information without the consent of the client.

See proposed Fin. Code § 4052(c). Similar language is found in H.R. 1636 (Stearns) — the "Consumer Privacy Protection Act of 2003".

What types of professional service providers, besides attorneys, would be covered by such a provision? There are many types of professionals who are subject to confidentiality requirements but who are not substantially engaged in financial activities and would not be subject to GLB in any event. Of those professionals who could be considered a financial institution within the meaning of GLB, the following appear to be subject to sufficiently strong confidentiality requirements that they arguably could be exempted under the SB 1 language:

- Attorney. See Bus. & Prof. Code § 6068(e).
- Paralegal. See Bus. & Prof. Code § 6453.
- ADR facilitator. See, e.g., Evid. Code §§ 1115-1128 (mediation confidentiality); AAA/ABA Code of Ethics for Arbitrators Canon VI.
- Certified public accountant. See Bus. & Prof. Code § 5037(a); 16 Cal. Code Regs. § 54.1; AICPA Code of Professional Conduct 01 Rule 301.
- Certified internal auditor. See IIA Code of Ethics.
- Certified financial planner. See FPA Code of Ethics and Professional Responsibility, Principle 5, Rule 501.
- Insurance professional. See Ins. Code § 791.13; 10 Cal. Code Regs. 2689.3.
- Real estate appraiser. See Bus. & Prof. Code § 11328; Uniform Standards of the Professional Appraisal Practice, Ethics Provision.
- Probate referee. See Prob. Code § 8908(a).

While a good case could be made that the activities listed above, and others, would come under the general exemption standards, it is not clear that they

would all be considered "professions" within the meaning of the proposed law. Does an insurance agency, for example, provide commercial services or professional services?

The defining characteristics of a profession are nebulous. The most comprehensive and compelling definition we have seen is spelled out in a 1974 New York case, *In re Freeman*, 34 N.Y.2d 1, 8-10, 311 N.E.2d 480 (1974). In discussing whether a statute regulating businesses was intended to reach the legal profession, the court, citing Roscoe Pound's *The Lawyer from Antiquity to Modern Times*, describes six criteria that define a profession:

(1) Extensive formal training and learning.
(2) Admission to practice by qualifying licensure.
(3) A code of ethics imposing standards qualitatively and extensively beyond those that prevail or are tolerated in the marketplace.
(4) A system for discipline of its members for violation of the code of ethics.
(5) A duty to subordinate financial reward to social responsibility.
(6) An obligation on its members, even in nonprofessional matters, to conduct themselves as members of a learned, disciplined, and honorable occupation.

Under these standards, very few of the "professions" identified above would qualify for exemption, for one reason or another. Some do not involve extensive formal training or learning, others do not require licensure, many are essentially engaged in trade or commerce unsubordinated to social responsibility.

Unless we make a specific listing of the professions that are exempted, there will always be uncertainty over whether a particular profession is covered. However, the staff does not think that a statutory listing of specific professions is desirable. Our search for covered professions would probably not be comprehensive, plus new professions evolve continually. Moreover, ethical standards and practices could change after enactment of the statute. The statute would be subject to perpetual amendment to list and delist covered professions.

A better approach may be to set out the general standard, and delegate to the state regulatory authority the determination of whether a particular profession falls within the exemption.

Exemption of certain professions

(a) This chapter does not apply to a member of a profession if the *state regulatory authority* determines that members of that

profession are prohibited from voluntarily disclosing confidential client information without the consent of the client.

(b) The *state regulatory authority* shall, on application of the governing body of a profession, determine whether this chapter applies to members of that profession under the standards provided in subdivision (a).

Comment. This section exempts a member of a qualifying profession from the requirements of this chapter, including notice requirements. The intent of the section is to delegate to the *state regulatory authority* the determination of whether confidentiality standards and enforcement for a particular profession are sufficiently strong that a member of the profession should be exempted form application of this chapter.

This section does not define "profession". The *state regulatory authority* may apply standards that appear appropriate to effectuate the principle purpose of this section, to exempt those activities where confidentiality requirements are so strong and so strongly enforced that application of this chapter would provide little or no added protection to the consumer.

The larger question is whether a provision such as this would withstand federal preemption. Under GLB, the FTC may determine that an inconsistent state law affords a consumer greater protection than GLB and therefore is not preempted by GLB. A state law that excuses an attorney or other professional from the duty of providing a privacy notice to clients might or might not be inconsistent with GLB's privacy notice requirement.

An argument could be made under classical preemption analysis that it is not impossible for an exempted professional to comply with both state and federal law, since the professional could give the privacy notice anyway, even though not required by federal law. But that doesn't accomplish much for the professional — the California law is not preempted, but the professional must still comply with federal privacy notice requirements.

Assuming that a state law providing such an exemption is determined to be inconsistent with GLB, could the state law nonetheless be considered more protective and therefore not preempted?

It is not clear whether FTC must look at individual provisions and determine whether each is more protective than GLB, or whether FTC may look at the state law taken as a whole and determine that on balance it is more protective than GLB. The regulations concerning preemption are silent on the matter. There is a suggestion in the FTC determination letter relating to North Dakota law that FTC

will look at individual provisions of state law, and that a general state opt in regime, while more protective of consumers than GLB, would not excuse compliance with GLB privacy notification requirements.

If we propose an exemption for certain professions, **we should also propose a severability clause**, so that invalidity of the exemption would not affect validity of the remainder of the statute. See discussion of "Retroactivity and Deferral of Operation" below.

Nonpublic Personal Information

Federal Definition

Recall that GLB regulates disclosure by financial institutions of "nonpublic personal information":

> (A) The term ''nonpublic personal information'' means personally identifiable financial information -
>
> (i) provided by a consumer to a financial institution;
>
> (ii) resulting from any transaction with the consumer or any service performed for the consumer; or
>
> (iii) otherwise obtained by the financial institution.
>
> (B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.
>
> (C) Notwithstanding subparagraph (B), such term -
>
> (i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but
>
> (ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

15 USC § 6809(4).

Personally identifiable financial information is defined in federal regulations. (In the regulations, "you" refers to the regulated financial institution.)

> (1) Personally identifiable financial information means any information:
>
> (i) A consumer provides to you to obtain a financial product or service from you;
>
> (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) Examples--

(i) Information included. Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet "cookie" (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) Information not included. Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

16 CFR 313.3(o).

Federal regulations also define "publicly available information", which a financial institution may disclose notwithstanding the fact that it is personally identifiable financial information:

(1) Publicly available information means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) Reasonable basis. You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) Examples--

(i) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(ii) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) Reasonable basis--

(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

16 CFR 313.3(p).

Information Provided by Consumer

The Commission has previously discussed the concept of nonpublic information that is personally identifiable, and the disclosure exception for publicly available information. One of the policy approaches considered by the Commission was to distinguish among sources of the information — if provided to a financial institution by the consumer it would be protected whether or not publicly available, and if obtained by the financial institution from public sources it would not be. The Commission decided to further research this matter, in particular with respect to the intent of GLB and implementing regulations.

GLB makes clear that it is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers'

nonpublic personal information. 15 USC § 6801(a). However, GLB also makes clear that it is not the intent of the law to limit disclosure of information that is otherwise public.

It would be possible to propose state legislation that would protect information provided by a consumer, whether or not that information is otherwise publicly available. So long as the California law is more protective of consumer privacy than GLB, it will not be preempted.

The staff does not see any real public policy benefit to a rule protecting information provided by a consumer, whether or not publicly available. We could not rely on that as a simple rule, since federal law also protects information gathered by a financial institution from other sources. To that extent, federal rather than California law would control, and the purpose of providing a single state rule would be frustrated.

Moreover, the staff does not see any significant policy argument that would support restricting the flow of publicly available information just because a consumer has included that information on a form submitted to a financial institution. Does it make sense to restrict a financial institution from using its own customers' publicly available information when no other financial institution or person in the state or country is restricted from using publicly available information concerning the customer?

There are information gathering practices that involve compiling a dossier from publicly available sources, and certainly some financial institutions take advantage of this. In practical terms, though, the greater use of the public information exception is likely to be as a defense to a claim of violation of a consumer's privacy protections. If the same information can be found in a public source, the financial institution will be free of liability for disclosing that information.

When a financial institution compiles information relating to its customers, does it segregate or label the information by source? If it has previously gathered public information about a consumer, is it thereafter precluded from using that information if the consumer discloses the same information on an application form to the financial institution?

Proposed Draft

The staff thinks **it will be easier and more understandable to all concerned simply to track the federal scheme** on this point. Again, it may be helpful to

have a state regulator acting as intermediary to provide guidance to businesses as federal regulations change and the meaning of state law changes with them. We suggest something like:

> **Scope of Chapter**
>
> (a) This chapter applies to disclosure of "nonpublic personal information" within the meaning of the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6809(4), and implementing regulations adopted pursuant to 15 USC § 6804.
>
> (b) The *state regulatory authority* shall by regulation elaborate the application of this chapter.
>
> **Comment.** The intent of this section is that the coverage of California's financial privacy protections be coextensive with the coverage of the Gramm-Leach-Bliley Act. Under federal law, "nonpublic personal information" is personally identifiable financial information provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution. 15 USC § 6809(4) (A).
>
> Federal regulations define personally identifiable financial information to include (1) information a consumer provides on an application to obtain a loan, credit card, or other financial product or service, (2) account balance information, payment history, overdraft history, and credit or debit card purchase information, (3) the fact that an individual is or has been a customer of or has obtained a financial product or service from a financial institution, (4) information about a consumer if it is disclosed in a manner that indicates that the individual is or has been a consumer of the financial institution; information that a consumer provides to a financial institution or that the institution or its agent otherwise obtains in connection with collecting on, or servicing, a credit account, (5) information a financial institution collects through an Internet "cookie" (an information collecting device from a web server), and(6) information from a consumer report. See, e.g., 16 CFR 313.3(o)(2)(i) (Federal Trade Commission regulations).
>
> Federal regulations exclude from "personally identifiable financial information" (1) a list of names and addresses of customers of an entity that is not a financial institution and (2) information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses. See, e.g., 16 CFR 313.3(o)(2)(ii) (Federal Trade Commission regulations).
>
> It should be noted that the term does not include publicly available information. That is information that a financial institution has a reasonable basis to believe is lawfully made

> available to the general public from (1) government records, such as real estate records and security interest filings, (2) widely distributed media, such as a telephone book, television or radio program, newspaper, or public web site, or (3) disclosures to the general public required to be made by law. See, e.g., 16 CFR 313.3(p) (Federal Trade Commission regulations).

OPT IN V. OPT OUT

Overview of Consumer Control

GLB limits the ability of a financial institution to share information about consumers with a nonaffiliated third party. A consumer must be given the ability to opt out of any information sharing by the financial institution with a nonaffiliated third party. Information sharing between divisions of the financial institution, or with its affiliates, is unrestricted.

The concept of an "affiliate" is central to the GLB regulatory structure. The reasoning goes something like this. In an era of financial supermarkets, a company that is organized with various divisions (e.g., separate departments for banking, insurance, and securities) may take information provided to one of its divisions by a customer and freely transfer that information to another of its divisions for marketing purposes. That gives a company with a divisional structure a significant marketing advantage over a comparable company that is organized in an "affiliate" structure.

In an affiliate structure, a holding company owns various businesses as separate entities rather than separate divisions within a single entity. GLB defines an affiliate organizational structure and allows sharing of information within that structure to the same degree that a company would be able to share that information internally among its divisions.

Some companies, though, are not large and are unable to provide the full range of financial services that a "financial supermarket" could provide. In order to compete effectively with the larger companies a smaller company must contract with nonaffiliated third parties to provide comparable financial services to its customers. Thus GLB allows sharing of information pursuant to a joint marketing agreement on the same basis that affiliate sharing is allowed to foster competition.

The only information subject to consumer control under GLB is sharing between a financial institution and a nonaffiliated third party with which the financial institution does not have a joint marketing agreement. And even in that

circumstance, GLB creates an exception for a third party that the financial institution uses for transactional purposes.

The enabling resolution for this study states a public policy to provide consumers greater control of their personal information. That could include control over information sharing among affiliates as well as with joint marketers. The control could take the form of an opt in (sharing prohibited unless affirmatively agreed to by the consumer) or an opt out (sharing allowed unless prohibited by the consumer).

This memorandum considers various issues surrounding information sharing within a financial institution, and with its affiliates, joint marketers, and transactional functionaries. It also examines the "marketing based" approach advocated by the Financial Services Privacy Coalition.

Divisional Structure

Why should a financial institution be permitted freely to share customer information among its various divisions?

Presumably, in many instances the information sharing will be for transactional reasons. But the fact that a customer has a deposit account with the banking division of a financial institution does not necessarily require that the financial institution should be free to share that customer's information with marketers in the insurance division.

If marketing is the main privacy concern, that concern would apply whether the marketing is done by a nonaffiliated third party, by a third party joint marketer, by an affiliated third party, or by another division of the same company.

The **staff does not recommend anything on this issue** at present. However, it is a consideration to bear in mind as we formulate our basic approach to the issues posed by the Legislature.

Affiliate Structure

GLB Treatment of Affiliates

What exactly is an affiliate? Under GLB an affiliate is a company that controls, is controlled by, or is under common control with, another company. 15 USC § 6809(6). "Control" is not defined by statute, but the regulations elaborate its meaning for purposes of GLB:

> Control of a company means:
>
> (1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
>
> (2) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or
>
> (3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

16 CFR 313.3(g).

While GLB permits free sharing of information among affiliates, SB 1 (Speier) would provide the consumer the right to opt out, as would S. 745 (Feinstein). What do other states do that have addressed the matter?

Most jurisdictions that have acted on the matter adopt the GLB approach, either by incorporating GLB by reference or by maintaining parallel statutory provisions. The law in these jurisdictions would not limit financial information sharing among affiliates.

A few states appear to go further and allow consumer control of affiliate sharing by requiring an opt in:

- North Dakota has an opt-in regime. A financial institution may not disclose customer information unless the disclosure is made pursuant to consent granted by the customer, in writing and signed by the customer. N.D. Cent. Code §§ 6-08.1-03 (duty of confidentiality), 6-08.1-04 (consent). See also N.D. Cent. Code § 6-08.1-02(11) (exemptions).
- Connecticut has an opt-in regime. Sharing of information with affiliates is subject to the Connecticut requirement. Conn. Gen. Stat. § 36a-42 (disclosure of financial records prohibited). However, the coverage of the Connecticut law is limited, applying only to disclosure of "financial records" (basically transactional information relating to a customer's deposit account) by a "financial institution" (basically a bank, credit union, or other depository — insurance companies and securities dealers are not covered). Conn. Gen. Stat. § 36a-41 (definitions).

What is the policy that supports special treatment of affiliates? If we accept the argument that a business that uses one form of organization should not be favored over an identical business that happens to use a different form of organization, it would seem to follow that a business using a divisional structure

should not be favored with respect to information sharing practices over a business that uses an affiliate structure. (Ignoring, for the moment, the larger question of why a business using a divisional structure should be allowed freely to share customer information internally among its divisions for marketing purposes.)

A business with divisions may be functionally the same as a business with affiliates. That assumes, of course, that the affiliates are wholly owned, just as divisions are wholly owned.

But GLB does not require 100% ownership. The regulation applies alternative tests of 50% control or 25% ownership, drawn from the Federal Reserve Act (12 USC 371c). In adopting this regulation, FTC considered the possibility of basing the concept of affiliation exclusively on ownership, but rejected that approach. "The Commission also believes that any test based only on stock ownership is unlikely to be flexible enough to address all situations in which companies are appropriately deemed to be affiliated and that including the stock ownership as one measurement of control provides necessary flexibility." 65 Fed. Reg. 33652 (May 24, 2000). The basis for this belief is not stated.

The Personal Insurance Federation of California has suggested to the Commission that for information sharing purposes, it may be appropriate to look at other possible distinguishing features among affiliates, such as:

- Financial affiliates versus nonfinancial affiliates.
- Affiliates in the same versus different lines of business (i.e., insurance/banks/securities).
- Affiliates offering functionally similar financial products.
- Affiliates regulated by the same functional regulator.
- Affiliates operating under a common brand name or through a common distribution system, such as through an agent or brokerage.

See letter attached to the First Supplement to Memorandum 2003-1 (Feb. 7, 2003).

The staff believes these are all interesting approaches and may be worth exploring, depending on how this project evolves. For now, **the staff would be reluctant to depart from the Commission's basic policy decision to track federal categories**. But because federal categories include a loose definition of what constitutes an affiliate relationship, that may influence the Commission's decision whether to give an affiliate preferential treatment for information sharing purposes.

In the meantime, a definition that tracks federal law would be consistent with the Commission's general approach on this project:

> **"Affiliate" defined**
>
> (a) As used in this chapter, "affiliate" has the meaning provided in the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6809(6), and implementing regulations adopted pursuant to 15 USC § 6804.
>
> (b) The *state regulatory authority* shall by regulation elaborate the meaning of the term "affiliate".
>
> **Comment.** The intent of this section is that the meaning of the term "affiliate" in California's financial privacy law be coextensive with the meaning of that term in the Gramm-Leach-Bliley Act. Under the Gramm-Leach-Bliley Act an affiliate is a company that controls, is controlled by, or is under common control with, another company. 15 USC § 6809(6). The regulations define control as:
>
> (1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
>
> (2) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or
>
> (3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.
>
> 16 CFR 313.3(g).

FCRA Treatment of Affiliates

FCRA regulates "consumer reports" — the communication of credit information about a consumer. FCRA excludes from the definition of consumer report any:

> (i) report containing information solely as to transactions or experiences between the consumer and the person making the report;
>
> (ii) communication of that information among persons related by common ownership or affiliated by corporate control; or
>
> (iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons.

15 USC § 1681a(d)(2)(A).

We have been unable to find any elaboration of the meaning of the term "affiliate" as used in FCRA, although that term is probably eclipsed by the concept of "related by common ownership" under FCRA. For these reasons, the **staff recommends that any Commission treatment of affiliates should employ the GLB definition**, without regard to possible FCRA nuances.

FCRA precludes a state from imposing a requirement or prohibition "with respect to the exchange of information among persons affiliated by common ownership or common corporate control." 15 USC § 1681t(b)(2). However, that prohibition ends January 1, 2004. Assuming there is no change in this situation as a result of congressional action, California should have a free hand in providing greater privacy protections on affiliate sharing than is available under FCRA, if it so desires. For further discussion, see "Federal Preemption" below.

Insurance Industry

The Personal Insurance Federation of California makes the argument that the insurance industry requires special treatment, regardless of general rules on information sharing among a financial institution's affiliates. That is because an affiliate structure is standard in the industry for legal and other reasons.

We have received a letter from the federation elaborating this argument. Exhibit p. 14. They point out that affiliate arrangements have historically prevailed within the insurance industry for a number of reasons. Initially the impetus was regulatory, due to prohibitions on an insurer engaging in more than one insurance line. Regulatory constraints still exist to some degree (cf. Ins. Code § 100), but multiple line insurance has become more common. Even multiple line insurers typically organize in an affiliate structure for purposes of compartmentalization of risk. That business structure better enables the insurer to satisfy underwriting, rating, capitalization, and reserve requirements applicable to each line of insurance, and protects policyholders in one line from catastrophic losses in another line.

Depending on the ultimate approach the Commission takes to affiliate sharing generally, the Commission should consider whether or not special treatment is indicated for the insurance industry.

Joint Marketing Agreements

GLB's joint marketing agreement provisions take internal sharing and affiliate sharing principles a step further. If information sharing is allowed freely within a company, or among a company's affiliates, that may give a larger company organized with divisions or affiliates a marketing advantage over a smaller company that must resort to joint marketing agreements with nonaffiliated third parties in order to offer financial products competitively.

GLB restricts information sharing by a financial institution with a nonaffiliated third party, except:

> This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.

15 USC 6802(b)(2).

The regulations give a broad meaning to the joint marketing exception — "For purposes of this section, joint agreement means a written contract pursuant to which ... one or more financial institutions jointly offer, endorse, or sponsor a financial product or service." 16 CFR 313.13(c).

Although the joint marketing exception is intended to level the playing field among larger and smaller competitors, there is no restriction either in GLB or in the implementing regulations on the size of an entity that may enter into a joint marketing agreement.

What have other jurisdictions done that have attempted comprehensive financial information regulation?

- North Dakota's opt in regime does not make an exception for joint marketing agreements; consumer consent would be required for disclosure of personal information to a joint marketer. See N.D. Cent. Code §§ 6-08.1-03 (duty of confidentiality), 6-08.1-04 (consent).

- The Connecticut opt in statute does not make an exception for sharing information pursuant to a joint marketing agreement. Conn. Gen. Stat. § 36a-42.
- The Illinois opt in statute does not make an exception for sharing information pursuant to a joint marketing agreement. Ill. Cons. Stat. § 5/48.1(c). However, Interpretive Letter No. 01-01 (March 9, 2001) of the Illinois Office of Banks and Real Estate concludes that, "Although Section 48.1 of the Act does not explicitly include these exceptions to its opt in requirement, the exceptions enumerated in the federal regulations are consistent with the purpose of Section 48.1 of the Act." Thus, a state bank need not obtain a customer's authorization to make a disclosure pursuant to a joint marketing agreement.
- Vermont has an opt in statute. 8 Vt. Stat. Ann. §§ 10203, 10204(2). Vermont banking regulations that implement the statute require an opt in for information sharing with nonaffiliated third parties, but the regulations create an exemption for joint marketing sharing Note, though, that the exemption is limited to sharing the consumer's name, contact information, and own transaction and experience information. Vt. Dept. of Bank., Ins., Sec. & Health Care Admin., Reg. B-2001-01 § 14.

SB 1 (Speier) would subject joint marketer sharing under California law to an opt out limitation, as would S. 745 (Feinstein) under federal law. The California Financial Privacy Act ballot initiative would subject all sharing of information to an opt in requirement; no exception would be made for affiliates or joint marketing agreements. The federal empirical study does not directly target joint marketing agreements, but it is possible it will include some information on their use and importance.

The purpose of the joint marketing agreement exception is to foster competition. If a large company is permitted to freely share information with affiliates, competition would be fostered by allowing a small company freely to share information with joint marketers.

The staff thinks that the joint marketing exception is so broad, it would cover essentially any activity a financial institution may be motivated to engage in. **The Commission should consider the possibility of limiting free sharing of information with affiliates, and a concomitant limitation on free sharing of information with joint marketers.** That will preserve privacy without giving a larger company a competitive advantage over a smaller one.

Nonaffiliated Third Parties

The one aspect of information sharing by a financial institution that GLB subjects to consumer control is sharing with a nonaffiliated third party (other than for joint marketing or transactional purposes). GLB requires a financial institution to provide notice to the consumer of its information sharing practices, and provide the consumer an opportunity to opt out. SB 1 (Speier) would prohibit information sharing of this type without the consumer's affirmative consent (opt in).

We do not have good information about the extent to which financial institutions transfer customer financial information to nonaffiliated third parties, and how significant a source of revenue this is. It is conceivable that the federal empirical study will provide some useful information, although that is not one of the points of inquiry in the study. We will collect further information on this matter before the conclusion of this study.

Apart from generalized privacy concerns about dispersion of personal information, there are two specific concerns generated by the sharing of information with a nonaffiliated third party. The first is harassment by marketers; the second is increased vulnerability to identity theft. Both will be addressed in the federal empirical study, which should illuminate both the benefits and detriments of nonaffiliated third party information sharing. The **staff recommends that the Commission continue to defer action** on this matter until the federal report is available.

Meanwhile, we have been informed that the dispersion of nonpublic personal information to third parties is not necessarily directly related to identity theft — it is the type of information transferred that is critical. For example, a person's account balance may not be helpful to an identity thief, whereas the person's social security number and account number would be.

GLB controls disclosure of account numbers, at least for marketing purposes:

> A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

15 USC § 6802(d).

With respect to social security numbers, S. 745 (Feinstein) would preclude the sale or purchase of an individual's social security number without the affirmatively expressed consent of the individual (opt in). See proposed 18 USC § 1028A(c). This general preclusion is subject to GLB:

> Nothing in this section shall prohibit or limit the display, sale, or purchase of social security numbers as permitted under title V of the Gramm-Leach-Bliley Act, or for the purpose of affiliate sharing as permitted under the Fair Credit Reporting Act, except that no entity regulated under such Acts may make social security numbers available to the general public, as may be determined by the appropriate regulators under such Acts. For purposes of this subsection, the general public shall not include affiliates or unaffiliated third-party business entities as may be defined by the appropriate regulators.

Proposed 18 USC § 1028A(f). Note, however, that S. 745 would also amend GLB to require an opt in for nonaffiliated third party sharing.

It appears to the staff that the only substantial reason for a financial institution to transfer information to a nonaffiliated third party, other than for transactional purposes (see discussion below), is that the information is valuable and can be a source of income to the financial institution. As a matter of public policy is this an interest that should be protected over the consumer's privacy interest? Note that there appears to be general agreement that the privacy interest deserves protection; the debate is whether opt out is sufficient for that purpose, or whether opt in should be required to protect the consumer's interest.

Facilitate Transactions

General Principle

The Commission has accepted the principle that the law should allow sharing of personal information for the purpose of facilitating the specific transaction requested by the consumer. This is the case under GLB, which also makes clear that there are other exceptions, such as to protect the security of records or for compliance with other laws:

> Subsections (a) and (b) of this section shall not prohibit the disclosure of nonpublic personal information -
>
> (1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with -
>
> (A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

(2) with the consent or at the direction of the consumer;

(3)(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(6)(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or (B) from a consumer report reported by a consumer reporting agency;

(7) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

15 U.S.C. § 6802(e).

There are, of course, federal regulations that elaborate these exceptions. For example:

> *Necessary to effect, administer, or enforce a transaction* means that the disclosure is:
>
> (1) Required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or
>
> (2) Required, or is a usual, appropriate or acceptable method:
>
> (i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the consumer's account in the ordinary course of providing the financial service or financial product;
>
> (ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;
>
> (iii) To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;
>
> (iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;
>
> (v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or State law;
>
> (vi) In connection with:
>
> (A) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means;
>
> (B) The transfer of receivables, accounts, or interests therein; or
>
> (C) The audit of debit, credit, or other payment information.

16 CFR 313.14(b) (Federal Trade Commission regulations).

Rather than parroting the detail of the federal regulations, the staff thinks **it is preferable to parallel the basic federal standard** and leave it to state regulatory authority to detail the meaning of some of the general standards.

Exceptions

This chapter does not prohibit disclosure of nonpublic personal information to the extent permitted by the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6802(e), and implementing regulations adopted pursuant to 15 USC § 6804.

Comment. The intent of this section is that the exceptions to California's financial privacy prohibitions be coextensive with the exceptions to the Gramm-Leach-Bliley Act.

Under federal law, 15 USC § 6802(e), a financial institution may disclose nonpublic personal information for the following purposes, regardless of a consumer's consent:

(1) As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with -

(A) servicing or processing a financial product or service requested or authorized by the consumer;

(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

(2) With the consent or at the direction of the consumer;

(3)(A) To protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

(4) To provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

(5) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-

regulatory organizations, or for an investigation on a matter related to public safety;

(6)(A) To a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or (B) from a consumer report reported by a consumer reporting agency;

(7) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(8) To comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

Additional State Exceptions

It is worth noting that SB 1 (Speier) would go beyond federal law and list a number of additional circumstances in which a financial institution may disclose nonpublic personal information of a consumer without the consumer's consent. These include:

- When a financial institution is reporting a known or suspected instance of elder or dependent adult financial abuse or is cooperating with a local adult protective services agency investigation of known or suspected elder or dependent adult financial abuse.
- The nonpublic personal information is released to identify or locate missing and abducted children, witnesses, criminals and fugitives, parties to lawsuits, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries, and missing heirs.
- The nonpublic personal information is released to a real estate appraiser licensed or certified by the state for submission to central data repositories such as the California Market Data Cooperative, and the nonpublic personal information is compiled strictly to complete other real estate appraisals and is not used for any other purpose.

It could be argued that at least some of these purposes fall within the catchall of GLB § 6802(e)(8), set out above. Compliance with "state or local laws, rules, and other applicable legal requirements" is a pretty broad standard. It is perhaps

useful to spell out some detail such as reporting of elder abuse or identification of missing children, but why these in particular? Undoubtedly these particulars have been brought to Senator Speier's attention by various public agencies or private interest groups that want to make clear the disclosures are allowed, and those particulars have been determined to be consistent with the general policy of the law.

But shouldn't this be done by regulation, if necessary, to clarify the many types of information disclosures that could come into question under the general standard. The determination of appropriate exceptions should not be left to the vagaries of particular issues that happen to come to the fore during the legislative process. **Regulations could collect the federal exemptions and set them out in one place**, readily accessible with the rest of state law.

> **Regulations detailing permitted disclosure of information**
>
> The *state regulatory authority* shall promulgate regulations that are consistent with federal law and that detail the disclosure of nonpublic personal information permitted pursuant to the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6802(e), and implementing regulations adopted pursuant to 15 USC § 6804.
>
> **Comment.** This section requires the *state regulatory authority* to collect the federal transactional exemptions and display them in regulation, together with state interpretation of the application of general federal standards. For example, federal law permits a financial institution to disclose nonpublic personal information without the consent of the consumer to comply with federal, state, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by federal, state, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law. See 15 USC § 6802(e)(8). Under this standard, the state regulatory might include in regulations, for example, a determination that the following disclosures are exempt:
>
> • Reporting a known or suspected instance of elder or dependent adult financial abuse or cooperating with a local adult protective services agency investigation of known or suspected elder or dependent adult financial abuse.
>
> • Reporting information for the purpose of identifying or locating missing or abducted children, witnesses, criminals and fugitives. or parents delinquent in child support payments.

Some of the statutory provisions for disclosure without the consumer's intent proposed by SB 1 would appear to go beyond the standard of federal law. For example, release of data to a real estate appraiser for submission to a data repository for use in other appraisals may be an admirable objective, but such a release would not appear to be otherwise required by state law. Since this portion of SB 1 would be less protective of financial privacy than GLB, it would arguably be preempted by federal law.

On the other hand, there is a kind of circularity to the GLB scheme. GLB limits disclosure of personal information, and preempts inconsistent state law. But GLB also permits otherwise prohibited disclosure of personal information if required by state law.

So arguably if state law provides for disclosure of real estate appraisal information, and if a financial institution complies with that provision, the GLB exemption for disclosures to comply with state law kicks in and state law overrides the general GLB privacy protection.

Of course, that analysis would make the GLB preemption provision a nullity, at least with respect to disclosure of information authorized by state law. We are not aware of any legal authority addressed to the point.

There are many laws that override privacy statutes for law enforcement and related purposes. It may be appropriate for proposed legislation to make clear that it is not intended to supersede overriding statutory provisions of this type. But should we make specific reference to these statutes, such as the USA Patriot Act? The staff thinks it would be better not to go down the path of listing individual statutes; where do we stop? Again, the staff believes that the state regulatory authority could provide a useful service by cataloguing overriding laws.

Marketing Based Approach

The Financial Services Privacy Coalition opposes SB 1 (Speier) for a number of reasons. A key problem, from the coalition's perspective, is that the bill regulates all sharing of nonpublic personal information by a financial institution. It weeds out permitted sharing on the basis of the business structure of the sharing entities. There is free sharing of information between divisions of a business. There is sharing subject to consumer opt out between affiliated businesses. And there is no sharing between nonaffiliated third parties unless the consumer opts in. But because many types of sharing between nonaffiliated third

parties are necessary for transactional and operational purposes, SB 1 catalogues and excepts them. The net result is that the whole scheme requires a financial institution to evaluate every information transaction in terms of the business structure of the parties involved and whether the transaction falls within one of the exceptions. According to the coalition, this is a costly and inefficient process that must be applied to millions of routine and reasonable information exchanges.

The coalition's proposal instead is to regulate only exchanges of information for marketing purposes. This would avoid the problems inherent in regulation of all information exchanges based on business structure and exceptions.

Presumably the coalition's proposal might look something like this (we do not want to put words in their mouth, but they have not provided us with proposed statutory language):

> **Limitation on information sharing for marketing purposes**
>
> A financial institution shall not transfer a customer's nonpublic personal information to a third party for marketing purposes unless the customer has consented to the transfer.

This sort of approach raises a number of issues of its own:

(1) How is "marketing purposes" defined? Suppose, for example, that a gun control group wants to target a certain population for petition circulation or political advertising. Are these marketing purposes? Must a financial institution make a determination of the intentions of the third party each time it transfers information.

(2) Are there any consequences to the financial institution if the third party to which the information is transferred uses it for marketing purposes?

(3) Does this unbalance the playing field in favor of businesses organized by divisions over those organized by affiliate structure and those that must resort to joint marketing agreements with third parties?

(4) What is the nature of the consent required — opt in or opt out?

(5) The approach is based on an assumption that consumers are only concerned about dispersion of their personal information for marketing purposes. But in fact they are also concerned about identity theft and general erosion of personal privacy, both of which may be aggravated by widespread dispersion of their personal information. The coalition approach does not appear to address those concerns.

(6) Would this approach avoid federal preemption? It would seem to be less, rather than more, protective of consumer privacy than GLB because of its narrower scope.

To the staff's mind, the major advantage this approach offers over SB 1 (and GLB) is that it avoids the need to catalog exceptions to the limitations on information sharing with nonaffiliated third parties. But whether this advantage outweighs the problems inherent in the approach is not clear.

It is also worth noting that Senator Feinstein's S. 745 adopts a marketing-based approach to information sharing by any commercial entity. As introduced, that bill would apply to disclosure of personal information to a nonaffiliated third party for marketing purposes. Pared down to its simplest form, the Feinstein bill provides:

> **Commercial sale and marketing of personally identifiable information**
> PROHIBITION
> (1) *In General*- It is unlawful for a commercial entity to collect personally identifiable information and disclose such information to any nonaffiliated third party for marketing purposes or sell such information to any nonaffiliated third party, unless the commercial entity provides--
> (A) notice to the individual to whom the information relates in accordance with the requirements of subsection (b); and
> (B) an opportunity for such individual to restrict the disclosure or sale of such information.
> (2) *Exception*- A commercial entity may collect personally identifiable information and use such information to market to potential customers such entity's product.
> DEFINITIONS
> *Marketing*- The term 'marketing' means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.
> *Personally Identifiable Information*- The term 'personally identifiable information' means individually identifiable information about the individual that is collected including--
> (A) a first, middle, or last name, whether given at birth or adoption, assumed, or legally changed;
> (B) a home or other physical address, including the street name, zip code, and name of a city or town;
> (C) an e-mail address;
> (D) a telephone number;
> (E) a photograph or other form of visual identification;

(F) a birth date, birth certificate number, or place of birth for that person; or

(G) information concerning the individual that is combined with any other identifier in this paragraph.

Sale; Sell; Sold- The terms 'sale', 'sell', and 'sold', with respect to personally identifiable information, mean the exchanging of such information for any thing of value, directly or indirectly, including the licensing, bartering, or renting of such information.

PRIVACY NOTICE

General Principles

The key to effective operation of an opt in or opt out scheme is the privacy notice. The privacy notice informs the consumer of the sorts of information sharing the financial institution may participate in, and provides the consumer the opportunity to exercise control. The pressures on the privacy notice differ with the type of consumer consent regime provided by law.

Suppose the law allows free sharing of information by a financial institution unless the consumer opts out. In that case, the financial institution may have an incentive not to make overly attractive to the consumer the opportunity to opt out. Financial institutions on the other hand point out that they have no interest in subjecting their customers to unwanted marketing information. It just wastes marketing resources, besides annoying their customers. Marketing is most effective when it is narrowly directed to a targeted population that is potentially receptive to the marketing message.

Suppose, on the other hand, the law requires a financial institution to obtain the consent of the consumer before it may share the consumer's personal information. In that case the financial institution may have an incentive to make the opt in opportunity clear and easily exercisable by the consumer. Or, it is possible that the financial institution may present the information in such a way that the consumer does not really understand what the consumer has consented to.

Contents of Notice

Does it make sense to try to prescribe by statute the contents of the notice, whether in an opt in or an opt out regime? GLB provides reasonable specificity concerning the contents of the required notice:

Disclosure of institution privacy policy

(a) Disclosure required

At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, of such financial institution's policies and practices with respect to -

(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 6802 of this title, including the categories of information that may be disclosed;

(2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and

(3) protecting the nonpublic personal information of consumers.

Such disclosures shall be made in accordance with the regulations prescribed under section 6804 of this title.

(b) Information to be included

The disclosure required by subsection (a) of this section shall include -

(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 6802 of this title, and including -

(A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to section 6802(e) of this title; and

(B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution;

(2) the categories of nonpublic personal information that are collected by the financial institution;

(3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 6801 of this title; and

(4) the disclosures required, if any, under section 1681a(d)(2)(A)(iii) of this title.

15 USC § 6803.

The implementing regulations address various aspects of the privacy notice. For example, GLB requires that the financial institution's disclosure of its privacy policy be "clear and conspicuous". The regulations state:

(1) Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples--

(i) Reasonably understandable. You make your notice reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible; and

(F) Avoid explanations that are imprecise and readily subject to different interpretations.

(ii) Designed to call attention. You design your notice to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

(iii) Notices on web sites. If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

16 CFR 313.3(b) (Federal Trade Commission).

The regulations also provide sample clauses that a financial institution may use, that constitute a safe harbor. Here is the sample opt out clause provided in the regulations:

> If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)"].

16 CFR Part 313, App. A (Sample Clause A-6).

Statutory Form

By way of comparison, SB 1 (Speier) would provide a statutory opt in or opt out form. Use of the prescribed form, or one that is substantially similar, is mandatory.

> IMPORTANT PRIVACY CHOICES FOR CALIFORNIANS
>
> California consumers have rights beyond those offered under federal law to control the sharing of some personal information by financial institutions. Please read the following information carefully before making your choices below. Consumers have the following rights to restrict the sharing of personal and financial information with affiliates (companies we own or control) and nonaffiliated third parties:
>
> SHARING INFORMATION WITH AFFILIATED COMPANIES: Unless you prohibit us from doing so, we may share personal and financial information about you with our affiliates.
> [ ] I prohibit you from sharing personal and financial information with affiliated companies.
>
> SHARING INFORMATION WITH FINANCIAL COMPANIES WITH WHOM WE CONTRACT: Unless you prohibit us from doing so, we may share personal and financial information about you with nonaffiliated financial companies with whom we contract to provide financial products and services.
> [ ] I prohibit you from sharing personal and financial information with financial companies with whom you contract to provide financial products and services.
>
> SHARING INFORMATION WITH NONAFFILIATED COMPANIES: Unless you authorize us to do so, we may not share personal and financial information about you with third party companies with whom we have not entered into a contract.
> [ ] I authorize you to share my personal and financial information with nonaffiliated companies.

I WANT TO RESTRICT THE SHARING OF MY INFORMATION TO THE GREATEST EXTENT ALLOWED BY LAW.
[ ] I prohibit you from sharing my personal and financial information with affiliates, nonaffiliated financial institutions, or other third parties. This may lead to my being offered fewer products and services.

Nothing in this form prohibits the sharing of information as necessary to administer your account or policy or as allowed by, or required to comply with, state or federal law, nor does it prohibit us from sending you information to market other products or services.

You may return this form at any time and your choices will remain in effect unless you request a change. However, if we do not hear from you within 45 days of sending this notice to you, we may share some of your information with affiliated companies and other nonaffiliated financial institutions with whom we have contracts.

Name: _____
Account or Policy Number(s): _____ (to be filled in by consumer)
Signature _____

To exercise your choices do one of the following:
(1) Fill out, sign, and send back this form to us using the envelope provided (you may want to make a copy for your records); (or)
(2) Call this toll-free number (800)xxx-xxxx or (xxx)xxx-xxxx; (or)
(3) Reply electronically by contacting us through the following Internet option: xxxx@xxx.

Should there be a statutorily required form as in SB 1, or should the matter be left to regulation as in GLB, with a safe harbor form available for use by a financial institution? The Commission has historically tried to avoid statutory forms, for various reasons, including the fact that lawyers are notoriously inept at drawing consumer friendly forms. Other reasons include the fact that the forms routinely are rendered inaccurate by a change in law that neglects to make a conforming change to the statutory form.

Staff Recommendation

The staff thinks **the regulatory approach is the better way to go**. Assuming the direction to the state regulatory authority is sufficiently clear as to the

governing standards, the state regulatory authority should be able to prescribe satisfactory forms, and improve them from time to time.

Should the forms be mandatory, or should they act as a safe harbor? The Commission generally tends to favor a safe harbor approach in comparable circumstances. No matter how good a regulator thinks the prescribed forms may be, a financial institution may be able to develop ones that better suit its own customers and circumstances. A financial institution will have an incentive to use safe harbor forms due to the liability risk if the financial institution violates statutory standards. See discussion of "Civil and Administrative Remedies" below.

We could also provide a regime that allows a financial institution to submit a proposed form to the state regulatory authority for a review and a determination whether it satisfies state standards (e.g., readability standards). One concern is that, given the very broad scope of this statute, the state regulatory authority would be overwhelmed by submissions from financial institutions.

Conversely, we also see merit in mandatory forms in this situation. There are so many of them coming from so many "financial institutions", with such a complex array of choices, that the ordinary consumer is overwhelmed. To the extent we can simplify matters and help understanding for everyone by providing a standardized form, that could be a significant benefit. On balance, we think **the mandatory approach is preferable** here.

Would prescription of a standard California form put an undue burden on a financial institution doing a national business to develop one form for GLB and a another form for California (and for every other state that decides to enact its own unique provisions)? Perhaps. But remember that the California law will be free of federal preemption only to the extent that it provides greater privacy protection for consumers than GLB, so the California privacy notice must at a minimum satisfy GLB standards. If we direct our state regulatory authority to meet those standards in formulating the form of the privacy notice, then a financial institution would at least have some assurance that it could use the California privacy form for GLB states as well.

> **Privacy notice**
>
> (a) A privacy notice required by this chapter shall provide the prescribed information to the recipient in a manner that facilitates understanding and informed exercise of choice, and shall at a minimum be clear and conspicuous within the meaning of the federal Financial Services Modernization Act (Gramm-Leach-Bliley

Act), 15 USC § 6803, and implementing regulations adopted pursuant to 15 USC § 6804.

(b) The *state regulatory authority* shall by regulation prescribe the form of privacy notices required by this chapter. Use of the form prescribed by regulation is mandatory.

Comment. Unlike federal law, which provides sample privacy notice forms, this section requires the *state regulatory authority* to promulgate mandatory privacy notice forms for use under this chapter that are at least as clear and conspicuous as those prescribed by federal law. Cf. 16 CFR §§ 313.3 ("clear and conspicuous" defined), 313.4-313.9 (privacy and opt out notices), and App. A (sample clauses).

The authority of the *state regulatory authority* to determine the form of a privacy notice is broad and would include authority to permit consolidation of privacy notices where appropriate.

As used in this section, "privacy notice" includes opt in and opt out notices as well as notices that disclose a financial institution's privacy policies and practices.

Note that this section does not address the content of a privacy notice. That we will prepare after we have made underlying policy decisions on opt in v. opt out, etc.

INTERSTATE COMMERCE

The Commission has noted the potential problem for a financial institution in complying with differing privacy regulations among the various states. The Commission requested information on experience under the federal Truth in Lending Act (Regulation Z), pursuant to which states have adopted variant disclosure requirements, which, though complex, have apparently not precluded businesses from operating satisfactorily.

The legal literature discloses few problems with Regulation Z compliance by businesses operating nationally. However, this may be in part attributable to a fairly aggressive posture towards preemption. Under Regulation Z, state law is preempted if it contains provisions inconsistent with federal law. Inconsistent state law would include:

- A law that requires a creditor to make a disclosure or take an action that contradicts federal requirements. A state law is considered contradictory if it uses terminology inconsistent with that used in federal law. (However, Regulation Z will tolerate a state disclosure requirement — other than one relating to a finance

charge, annual percentage rate, or other specified disclosures — on a determination by the Federal Reserve Board that the state disclosure is substantially the same in meaning as a federal disclosure.)

- A law that provides rights, responsibilities, or procedures for consumers or creditors that differ from those required by federal law. (However, Regulation Z specifically allows a state law with a longer time limit for inquiries relating to an open-end credit account, subject to specifically required disclosures.)
- A law relating to disclosure of credit information in a credit or charge card application or solicitation or renewal notice.

See 12 CFR 226.28.

There is an implication in the literature that the aggressive preemption posture of Regulation Z is the result of unsatisfactory experience with an earlier version of the preemption regulation. Under the old regulation, a looser preemption standard applied to state law that imposed requirements "different from the requirements of [Regulation Z] with respect to form, content, terminology, or time of delivery." The Federal Reserve Board tightened up the preemption requirements as part of the Truth in Lending Simplification Act. *Compare* Prior Regulation Z, 12 C.F.R. § 226.6(b)(1) (repealed as of Oct. 1, 1982) *with* Regulation Z, 12 C.F.R. § 226.28(a)(1) (1984).

GLB's preemption approach is more liberal than that under Regulation Z, so it is not clear that the favorable Regulation Z experience is instructive, other than perhaps to suggest that a more aggressive approach to preemption may be called for. And as we know, measures have now been introduced in Congress to reverse the current pattern and provide for GLB and FCRA preemption of state law. See discussion of "Current Developments" above.

For now, the Commission has decided as a matter of general policy that state law should seek to track federal definitions, categories, and concepts, so as to facilitate compliance by financial institutions. This we have tried to do in the various drafts set out in this memorandum. In particular, we have tried to ensure that governing federal regulations are tracked as well as statutory language.

INTERNATIONAL COMPETITION

The Commission has decided that as a general policy, it will seek to propose statutory regulation that would be not inconsistent with foreign regulation , so as

to facilitate the ability of entities doing business in California to be competitive in international commerce.

The "EU Safe Harbor" was developed by the U.S. Department of Commerce, so that a domestic company that subscribes to the safe harbor principles may be assured of compliance with European privacy directives. GLB satisfies the EU Safe Harbor principles, as would any legislation recommended by the Commission. Key provisions of the safe harbor include notice to consumers and an opportunity to opt out with respect to sharing of personal information.

> NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).
>
> CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.
>
> It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

Canada has legislation for the protection of personal information in the private sector, the Personal Information Protection and Electronic Documents Act, Stat. Canada, 48-49 Eliz. II, Ch. 5 (2000). That legislation is generally consistent with the EU Safe Harbor. It adopts the principles set out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information (Schedule 1). The principles provide for notice and an opportunity to opt out. For example, the "Consent" principle requires:

4.3 Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take

into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8

> An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

GLB is not inconsistent with these principles, nor is any legislation recommended by the Commission likely to be.

CIVIL AND ADMINISTRATIVE REMEDIES

The enabling resolution for this study directs the Commission to recommend legislation that will:

> Provide for civil remedies and administrative and civil penalties for a violation of the recommended legislation, including, but not limited to, attorney's fees, costs, actual and compensatory damages, and exemplary damages, including, but not limited to, relief as provided pursuant to Article 3 (commencing with Section 3294) of Chapter 1 of Title 2 of Part 1 of Division 4 of the Civil Code, and as provided in unfair business practices actions brought under Article 1 (commencing with Section 17000) of Chapter 4 of Part 2 of Division 7 of the Business and Professions Code.

2002 Cal. Stat. res. ch. 167.

Civil Remedies

Cause of Action

What should be actionable — willful disclosure, certainly, but what about negligent disclosure (e.g., clerk inadvertently attaches wrong document to email, or hacker gets access to improperly protected data base)? While it is incumbent on a financial institution in possession of personal information to adequately protect the security of that information, the staff thinks that issue is really beyond the scope of the present study.

Other types of negligent disclosure, however, we might want to address. Suppose a consumer opts out of disclosure, but the financial institution is slow to act on that information, resulting in unwarranted disclosures of that consumer's information. Or the financial institution fails properly to train its clerical staff or properly to program its computers, with the result that the consumer's personal information continues to be disclosed through the negligence of the financial institution. Is the financial institution culpable in those circumstances, or should

we limit ourselves here to intentional violations of the statutory duty? Some behavior may be so grossly negligent that it should be considered willful.

Suppose the financial institution releases information without properly notifying the consumer or without honoring the consumer's request not to disclose personal information. Does the consumer have a separate cause of action for each person to whom the information is released? Is there a separate cause of action for each item of information released? Suppose the financial institution improperly releases a second set of information to the same recipient a month later with basically the same information, only updated or errors corrected — is that two separate causes of action? What about technical violations — the financial institution gives the required notice, but neglects to include one of the mandated disclosures that doesn't happen to apply to the circumstances of a particular consumer anyway? The issues are innumerable.

To some extent these issues only become important if a civil penalty is assessed. If the exclusive remedy were actual damages, many of these questions would become nonissues — separate or sequential releases of information would become important only if they were the cause of increased harm to the consumer.

On the other hand, if a civil penalty is assessed, then it becomes a question whether the penalty is assessed for each disclosure, for each recipient, for each item of information released, etc. This is more than an academic discussion, since the staff believes that a civil penalty may be the only practical remedy for the ordinary consumer, and in fact the only realistic means of enforcing the privacy law in an era of limited public funding for administrative enforcement remedies. See discussion below.

Measure of Damages

What is the measure of damages suffered by a consumer if a financial institution fails to give the privacy notice or gives an insufficient notice, or if the financial institution improperly discloses the consumer's nonpublic personal information to a nonaffiliated third party? Should liability depend on whether the failure is intentional or negligent? How will a consumer obtain proof that a financial institution has actually disclosed personal information without consent (as opposed to a third party obtaining that information by illicit means)? What consumer can realistically afford the cost of litigation so that civil liability is an effective remedy?

The answers to these questions are at least partially suggested in the enabling resolution for this study — there may be a role to play here for civil penalties, as well as for exemplary damages and attorney's fees. Also, if we keep remedies within the jurisdiction of the small claims division of the superior court, the remedies may be more practical for the ordinary consumer.

While administrative remedies might be more effectual than civil remedies, realistically in an era of reduced funding for state operations consumers may have to be self reliant in enforcement of their privacy rights.

The staff notes that SB 1 (Speier) would assess a civil penalty not to exceed $2,500 per violation, with the amount doubled if the violation results in identity theft. That amount is significant enough to act as a deterrent, yet remains within the small claims court jurisdiction. SB 1 requires the court to take a number of factors into account in setting the amount of the penalty:

> In determining the penalty to be assessed pursuant to a violation of this division, the court shall take into account the following factors:
>
> (1) The total assets and net worth of the violating entity.
>
> (2) The nature and seriousness of the violation.
>
> (3) The persistence of the violation, including any attempts to correct the situation leading to the violation.
>
> (4) The length of time over which the violation occurred.
>
> (5) The number of times the entity has violated this division.
>
> (6) The harm caused to consumers by the violation.
>
> (7) The level of proceeds derived from the violation.
>
> (8) The impact of possible penalties on the overall fiscal solvency of the violating entity.

Proposed Fin. Code § 4057(c).

But why not eliminate the court's discretion, and simply **provide a smaller but automatic civil penalty in a flat amount, or actual damages, whichever is greater**? The staff suggests a flat penalty of $500 per occurrence. That would apply any time information is released in violation of the statute. For example, if a financial institution has a contract with a third party to provide the third party a monthly customer list and if a customer's name is improperly included on the list that is disclosed to the third party, over the course of a year there would be 12 violations of the statute, resulting in an annual civil penalty of $6,000. The $500 amount should be sufficient to deter a financial institution as well as to provide the consumer an enforcement incentive.

Exemplary Damages

The Commission is instructed to include in its consideration of civil remedies exemplary damages, "including but not limited to" relief as provided in Article 3 (commencing with Section 3294) of Chapter 1 of Title 2 of Part 1 of Division 4 of the Civil Code. That statute provides a scheme for the plaintiff to recover, in addition to actual damages, damages for the sake of example and by way of punishing the defendant.

It is not uncommon to find an allowance of punitive damages in invasion of privacy cases. See, e.g., Civ. Code § 17608.8(c) (punitive damages for invasion of privacy subject to proof under Section 3294); *Diaz v. Oakland Tribune*, 139 Cal. App. 3d 118, 188 Cal. Rptr. 762 (1983) (punitive damages in common law action subject to showing of malice). The Civil Code statutory scheme for exemplary damages requires proof by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice.

California statutes on confidentiality of medical information provide expressly for recovery of punitive damages by a patient whose medical information has been used or disclosed in violation of specified statutes and who has sustained economic loss or personal injury as a result. The punitive damages may not exceed $3,000. Civ. Code § 56.35.

The staff sees no reason why the general punitive damages statute should not be adequate for our present purposes. No special provisions are necessary. **We would simply cross-refer to the exemplary damages statute in the Comment.**

Costs and Attorney's Fees

With respect to attorney's fees, there are a number of practicalities to consider. If attorney's fees are not allowed, that will serve as an inducement to resolve these disputes using the small claims procedure. But in a case where damages exceed the small claims jurisdiction, it may be impossible for the ordinary consumer to get recompense without an allowance of attorney's fees. But allowing attorney's fees may encourage a consumer to invoke limited civil case procedures even where small claims procedures would be more appropriate.

The staff sees a couple of promising approaches here. We could allow attorney's fees but invoke the provision of Code of Civil Procedure Section 1033(b)(1) that allows the court to deny costs if the case could have been brought in small claims court and the recovery is within the small claims jurisdiction. Cf.

Dorman v. DWLC Corp., 35 Cal. App. 4th 1808, 42 Cal. Rptr. 2d 459 (1995) (statute covers attorney's fees). Or we could **allow attorney's fees to the prevailing party**, not just to the plaintiff. The staff prefers the latter approach since it will have a tendency to restrain potentially frivolous or harassing lawsuits.

Statute of Limitations

The ordinary statute of limitations for an action on a statutory liability is three years. Code Civ. Proc. § 338(a). The ordinary statute of limitations for an action on a statutory penalty is one year. Code Civ. Proc. § 340(a). Given the dynamics of the financial services industry and the timing of when privacy violations are likely to surface and any identity theft problems played out, a middle ground of a **two year limitations period for both remedies** appears appropriate to the staff.

The staff draft set out below would run the limitations period from disclosure, rather than discovery. This will avoid the problem of an intangible violation of the statute, with no apparent harm but subject to a statutory penalty, remaining actionable if it comes to light many years after the violation occurred.

Unfair Competition Litigation

The enabling resolution for this study directs the Commission to consider the availability of relief in an unfair business practices action, Article 1 (commencing with Section 17000) of Chapter 4 of Part 2 of Division 7 of the Business and Professions Code. The staff assumes this statutory reference is erroneous, since the article referred to merely states the general purpose of the Legislature to safeguard the public against monopolies and to foster and encourage competition among businesses by prohibiting unfair practices. The Unfair Practices Act (found at Business and Professions Code Sections 17000-17101) is to be distinguished from the problematic Unfair Competition Law (found at Business and Professions Code Sections 17200-17210), although as we shall see, there is a connection between the two.

The Unfair Practices Act is aimed at anticompetitive activities such as lowering prices in a particular market or selling at below cost or as a "loss leader", with the intent to destroy competition. Bus. & Prof. Code § 17040-17051. Presumably anticompetitive activity in the financial privacy area would involve a financial institution's improper use of personal information of a customer to give the financial institution and its affiliates and joint marketers an unfair advantage over business competitors.

Remedies for violation of the Unfair Practices Act can be quite severe, including both civil and criminal remedies. Civil remedies include injunctive relief, treble damages, and costs and attorney's fees. Bus. & Prof. Code §§ 17070-17087. In addition violation of the statute is a misdemeanor. Bus. & Prof. Code §§ 17100-17101.

By way of contrast, remedies under the Unfair Competition Law (Bus. & Prof. Code § 17200 et seq.) exclude damages but include civil penalties and restitution. The remedies under that statute are powerful because the statute permits class action-like proceedings on behalf of the general public. In addition, the remedies and penalties under that statute are cumulative with the remedies and penalties under other laws.

Thus a violation of the Unfair Practices Act would also be actionable under the Unfair Competition Law. Moreover, the Unfair Competition Law provides an independent cause of action for "any unlawful, unfair or fraudulent business act or practice" (Bus. & Prof. Code § 17200), which may cover conduct otherwise proper under the Unfair Practices Act.

The interrelation between the two statutes and their remedies is explored at some length in *Cel-Tech Communications v. L.A. Cellular*, 10 Cal. 4th 163, 83 Cal. Rptr. 2d 548, 973 P. 2d 527 (1999). The court concludes in that case that a violation of the Unfair Practices Act would be actionable under the Unfair Competition Law unless relief under that statute is specifically barred, or the complained of conduct specifically authorized, by statute.

> This conclusion is consistent with the overall pattern of the Unfair Practices Act and the unfair competition law. As discussed above, the Unfair Practices Act condemns specific conduct. The unfair competition law is less specific, because the Legislature cannot anticipate all possible forms in which unfairness might occur. If, in the Unfair Practices Act (or some other provision), the Legislature considered certain activity in certain circumstances and determined it to be lawful, courts may not override that determination under the guise of the unfair competition law. However, if the Legislature did not consider that activity in those circumstances, the failure to proscribe it in a specific provision does not prevent a judicial determination that it is unfair under the unfair competition law.

83 Cal. Rptr. 2d at 563.

Thus, if the Commission wishes to authorize relief under the Unfair Practices Act as suggested by the Legislature, but not thereby trigger a Section 17200

action, express language to that effect must be included in the proposed legislation. The reason the Commission might want to preclude relief under Section 17200 is because of the well-documented potential for abuse under that statute. It should be noted, however, that a dozen bills have been introduced this session to reform the Section 17200 procedure, many of them picking up various aspects of the procedural reforms proposed by the Commission. See, e.g., AB 69 (Correa). One approach the Commission might take would be tentatively to **preclude Section 17200 relief, but monitor progress on Section 17200 reform** and revisit the issue at the end of the current legislative year.

In any event, is relief under the Unfair Practices Act for a privacy violation necessary or desirable? To a large extent remedies under that act overlap the damages and attorney's fee sanctions that we are already looking at for privacy violations. The **treble damages and criminal sanctions allowed under the Unfair Practices Act seem extreme** — they are really designed to punish predatory business practices engaged in for the purpose of eliminating competition.

Preemption Issues

GLB provides no civil remedies, only administrative enforcement. 15 USC § 6805. FCRA provides civil as well as administrative remedies. 15 USC §§ 1681n-1681s.

The staff does not believe state civil remedies would be preempted by GLB. Since GLB does not preempt state law except to the extent state law is inconsistent with GLB, and since the policy of GLB is to protect the privacy of consumers, it is likely that state civil remedies for privacy violations would be held to be consistent, rather than inconsistent, with GLB and, even if inconsistent, would be held to provide greater privacy protection.

In at least two cases federal courts have found state civil remedies preempted by FCRA. See *Elliott v. TRW*, 889 F. Supp. 960 (ND Texas 1995) (defamation claim); *Retail Credit Co. v. Dade County, Fla.*, 393 F. Supp. 577 (S.D. Fla. 1975) (qualified immunity from suit for defamation, invasion of privacy, and negligent disclosure). The rationale is that FCRA provides a qualified immunity from common law causes of action for matters governed by FCRA; state law imposing a common law cause of action is therefore inconsistent with FCRA. (Whether this analysis would be the same after January 1, 2004, is unknown. See discussion of "Federal Preemption" below.)

Draft Statute

Putting together the various suggestions made above, a draft civil remedy statute might look something like this:

> **Civil remedy**
>
> (a) This section applies to a willful, or grossly negligent, disclosure by a financial institution of nonpublic personal information of a consumer without the consent of the consumer required by this chapter. Each separate transmission of nonpublic personal information by a financial institution to an unauthorized person is a separate disclosure of that information for purposes of this section.
>
> (b) A financial institution is liable to the consumer for damages caused by a disclosure of the consumer's nonpublic personal information described in subdivision (a). The damages recoverable under this section are the greater of:
>
> (1) Actual damages resulting from the disclosure, including but not limited to the nuisance cost of unsolicited marketing and the time, expense, and emotional cost of any identity theft resulting from the disclosure.
>
> (2) A civil penalty of $500 for the disclosure.
>
> (c) The prevailing party in an action under this section is entitled to recover litigation expenses, including court costs and a reasonable attorney's fee.
>
> (d) An action under this section shall be commenced within two years after the disclosure of the consumer's nonpublic personal information.
>
> (e) The remedies provided in this chapter are cumulative to each other but are exclusive of the remedies or penalties provided in Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code.
>
> **Comment.** This section prescribes civil remedies for improper disclosure of nonpublic personal information by a financial institution. For administrative remedies see Section [*administrative enforcement*].
>
> Under subdivision (a), there is a separate cause of action for each separate improper disclosure of nonpublic personal information, whether the disclosure is to the same person or a different person, and whether of the same information or different information.
>
> Subdivision (b) limits the causes of action for which damages are recoverable under this section to violations of the disclosure provisions of this chapter. Violations of notice or other provisions of this chapter are subject to administrative, rather than civil, remedies.

Subdivision (d) provides a statute of limitations running from disclosure, rather than discovery. The special statute applies notwithstanding the general three year statute for an action on a statutory liability (Code Civ. Proc. § 338(a)) and the general one year statute for an action on a statutory penalty (Code Civ. Proc. § 340(a)).

Subdivision (e) precludes action for a violation of this chapter under the Unfair Competition Law, Business and Professions Code Section 17200 et seq. However, nothing in this section limits the availability of supplemental relief under other provisions of law where appropriate, including but not limited to Article 3 (commencing with Section 3294) of Chapter 1 of Title 2 of Part 1 of Division 4 of the Civil Code (exemplary damages).

Administrative Penalties

Administrative enforcement of the privacy statute could perhaps be more efficacious than private enforcement. However, in the state's current tight budget situation, there will not be sufficient funds for an active enforcement program. But if we give the statute regulatory authority the necessary tools, the tools will be available when the opportunity for action comes.

The enabling resolution for this study contemplates enforcement by "administrative penalties" among other remedies. The staff does not think that the state regulatory authority should be limited to imposition of a monetary penalty. Other **traditional administrative sanctions, such as a cease and desist order, may be more effective in halting statute violations** and may be preferable. The staff would provide the ordinary range of administrative remedies for violation of the privacy statute.

Administrative enforcement

(a) The *state regulatory authority* may enforce compliance by a financial institution with the duties prescribed in this chapter. Administrative remedies under this chapter include but are not limited to discovery orders, subpoenas, and cease and desist orders.

(b) The orders of the *state regulatory authority* are judicially enforceable. The *state regulatory authority* may maintain a civil action on behalf of the public for violation of the duties prescribed in this chapter. The *state regulatory authority* may refer a financial institution that persistently or egregiously violates this chapter to the functional regulator of that financial institution for licensing action or other regulatory discipline.

(c) The administrative remedies provided in this section are cumulative to each other and to the civil remedies provided in this chapter for disclosure by a financial institution of nonpublic

personal information of a consumer without the consent of the consumer required by this chapter.

Comment. Subdivision (a) of this section authorizes a wide range of administrative enforcement actions for a violation of this chapter. It should be noted that the administrative enforcement authority under this chapter extends to any violation of the chapter, including a failure to comply with privacy notice requirements. Compare Section [*civil remedies for unauthorized disclosure of nonpublic personal information*]. Nothing in this section precludes both civil and administrative remedies for unauthorized disclosure. Subdivision (c).

This section does not provide for administrative fines. However, under subdivision (b) the *state regulatory authority* may bring an action for a civil penalty on behalf of a member of the public.

JURISDICTIONAL ISSUES

The enabling resolution for this study states that the objective of the study is to protect the privacy rights of "citizens of California". 2002 Cal. Stat. res. ch. 167.

To whom can or should the protection of California financial privacy law extend? A domiciliary? A resident? A transient who enters into a financial transaction in California (e.g., a credit card purchase)? Suppose a Californian enters into a financial transaction in another state (e.g., establishes a bank account), but maintains a continuing relationship with the out of state financial institution? Suppose a non-Californian establishes a financial relationship in another state but subsequently moves to California? Does it make a difference whether the out of state financial institution also does business in California?

The permutations are endless, and both log arm jurisdiction and choice of law rules may vary significantly depending on a host of imprecise factors, including minimum contacts, doing business in the state, traditional notions of fair play and substantial justice, and the like. There are practical considerations as well — if a customer of a financial institution moves to California, must the financial institution thereupon provide the customer the California privacy notice? How does the financial institution know whether the customer has actually moved or is just spending time here? If the customer has actually moved, how much time does the financial institution have to come into compliance with California law before it becomes liable for violating the customer's California privacy rights? Does the financial institution remain subject to the privacy laws of the

jurisdiction where the customer relationship was established? What are the governing conflict of laws principles here?

This area of law is complex because it does not focus on a single transaction, but deals with ongoing duties among the parties. And while personal information of a consumer may be collected or generated in the course of a financial transaction, it is not necessarily clear where the transaction may be said to have taken place. (Take for example a credit card purchase entered into by a California consumer in Oregon, charged to a credit card account serviced in Nevada, pursuant to a credit arrangement with a South Dakota corporation, but contractually agreed to via a website on the internet.) In a sense "property" is involved as well (the customer's personal information), but the property is intangible and does not have an identifiable location (or may have multiple locations). As a consequence, the law in this area defies standard categories.

The staff thinks that in order to make sense out of the whole thing and make the law workable, we should not overreach. California should seek to regulate those financial relationships in which the state has a substantial interest. This is particularly important because of the breadth of transactions that could be considered "financial" under GLB.

SB 1 (Speier) includes well articulated jurisdictional provisions. It would apply to a financial institution "doing business in this state" with respect to a consumer "resident of this state". Proposed Fin. Code § 4052(c), (f). The proposal also includes guidance for a financial institution to determine whether a consumer is a resident of California:

> For purposes of this division, an individual resident of this state is someone whose last known mailing address, other than an Armed Forces Post Office or Fleet Post Office address, as shown in the records of the financial institution, is located in this state. For purposes of this division, an individual is not a consumer of a financial institution solely because he or she is (1) a participant or beneficiary of an employee benefit plan that a financial institution administers or sponsors, or for which the financial institution acts as a trustee, insurer, or fiduciary, (2) covered under a group or blanket insurance policy or group annuity contract issued by the financial institution, (3) a beneficiary in a workers' compensation plan, (4) a beneficiary of a trust for which the financial institution is a trustee, or (5) a person who has designated the financial institution as trustee for a trust, provided that (A) the financial institution provides all required notices and rights required by this division to the plan sponsor, group or blanket insurance

> policyholder, or group annuity contractholder and (B) the financial institution does not disclose to any affiliate or any nonaffiliated third-party nonpublic personal information about the individual except as authorized in Section 4056.

Proposed Fin. Code § 4052(f).

The **staff is not prepared at this point to make definitive recommendations** to the Commission with respect to jurisdictional issues. However, to stimulate and provoke consideration of alternatives, the staff offers the following thoughts:

(1) *Doing business in the state.* California law could seek to control personal information obtained in connection with or arising out of a financial transaction entered into in this state. This is a commonly used term for regulatory purposes, and provides a due process nexus for the state to assert enforcement jurisdiction. The meaning of the term may be in flux as technology changes the manner in which business is done remotely. But that is a general problem, and as the law struggles to accommodate technology, the financial privacy statute would keep pace with the evolving law. Would this be a more or less useful focus of regulatory activity than the general "doing business in this state" standard?

(2) *Resident in this state.* California law could be made to apply to transactions entered into in this state regardless of the residence of the consumer. The residential status of a California consumer can change. If the consumer moves out of California, should the financial institution be free of California privacy constraints? If the consumer moves into California, should the financial institution become subject to California's privacy constraints? If we were to apply California privacy protections to information arising from transactions entered into in California, would that unduly burden California courts and regulators for the benefit of nonresidents?

(3) *Choice of law*. Suppose a financial institution would rather not be bound by California privacy controls and adds to its California contracts a clause to the effect that privacy rights under the contract are to be governed by Nevada law. Would public policy prohibit this, if the consumer freely and knowingly agreed to it? Presumably standard unconscionability doctrine could be applied here.

(4) *Waiver of rights*. An analogous question, not strictly jurisdictional, is whether a financial institution may include in its California contracts a provision that the consumer waives any required privacy notice and any opt in or opt out opportunities. Because this is a consumer transaction and the law implements an important public policy, the statute perhaps should preclude advance waiver of

rights. Should we force a consumer to receive privacy notices even if the consumer does not care about privacy issues?

FEDERAL PREEMPTION

State Statutes

General Considerations

If California enters this field, the staff thinks it is important that the state occupy it completely, and not be preempted by any aspect of federal law. The body of law is complex enough as it is, without a business having to cope with two bodies of parallel but variant provisions, some of which may apply in some circumstances and some in others.

The general federal policy, expressed both in GLB and in FCRA, is that federal law will not preempt inconsistent state privacy laws to the extent those laws are at least as protective of consumer privacy as federal law. See 15 USC § 6807 (GLB relation to state laws); 15 U.S.C. § 1681t(b)(d)(2) (FCRA relation to state laws).

In light of this, the staff thinks **it is important that state law not codify the text of governing federal regulations** on financial privacy. If the federal regulations change to provide greater privacy protection, inconsistent state law would be preempted until it is conformed. Federal law would control meanwhile, creating confusion for a financial institution that relies on California law (and on any previous determination of non preemption).

In this memorandum, the staff has generally followed an incorporation by reference approach, supplemented by an instruction to the state regulatory authority to flesh out the bare bones statute with regulatory detail that parallels the federal law, including regulations. A general instruction to the state regulatory authority would be helpful:

> **Consistency with Federal Law**
>
> If a provision of this chapter incorporates by reference a federal statute and regulations, the *state regulatory authority* shall by regulation adopt the applicable federal statute and regulations as state regulations. The *state regulatory authority* shall revise the state regulations as necessary to keep them in conformity with federal law.
>
> **Comment**. Various provisions of this chapter incorporate by reference federal law. See, e.g., Sections [*here collect and describe provisions that incorporate by reference*] "financial institution" defined;

> "nonpublic personal information" defined. The purpose of this section is to bring the governing federal statute and regulations into the corpus of state law by replicating them in state regulations, accessible in state law to persons affected by them. To the extent there is a discrepancy between federal law and the state regulations purporting to adopt federal law, federal law controls.

GLB Preemption

A key concept in the preemption equation is that of "inconsistency." A state statute may differ from federal law without being inconsistent. So long as there is no inconsistency, there is no danger of preemption. It is only where a state law is inconsistent with federal law under GLB and is potentially preempted that it becomes necessary to determine whether or not the state law provides greater privacy protection than GLB.

A state law is inconsistent if it frustrates the purpose of the federal regulatory scheme or if it makes compliance with both state and federal laws physically impossible. See, e.g., *English v. General Elec. Co.*, 496 U.S. 72, 78-79 (1990). Is there any prospect that the state privacy law we are crafting could be found to be inconsistent with GLB?

Of the two state preemption determinations by FTC to date — North Dakota and Connecticut — neither state statute was found to be inconsistent with GLB. However, North Dakota did not provide a good test since the statute had been amended to exempt from state law any financial institution that complies with GLB.

Connecticut provided a better test, since Connecticut law requires a customer's opt in for disclosure of certain financial records by certain financial institutions. Conn. Gen. Stat. §§ 36a-41, 42. The FTC concluded that this law does not frustrate the purpose of GLB to protect consumer financial privacy. Moreover, it is not physically impossible to comply with both Connecticut law and GLB since a Connecticut financial institution could comply with both by not disclosing a consumer's nonpublic personal information. Therefore FTC concluded that Connecticut law is not inconsistent with GLB, and it is unnecessary to engage in a "greater protection" analysis.

At this point it is not possible to determine whether any legislation we may propose will be inconsistent with GLB in the sense of either frustrating its purpose or making it physically impossible to comply with both state law and GLB. If there is any possibility that the legislation could be considered

inconsistent, it will be important to obtain an FTC determination up front that there is no federal preemption under GLB because state law provides greater privacy protection. The staff does not believe it is acceptable simply to allow a questionable California law to go into effect, and leave it to the affected parties to fight out the preemption issue in court.

In fact, as the staff reads federal law, it would preempt an inconsistent state statute under GLB by operation of law until an FTC determination is obtained:

> **Relation to State laws**
> *(a) In general*
> This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.
> *(b) Greater protection under State law*
> For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, **as determined by the Federal Trade Commission**, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.

15 USC § 6807 (emphasis added).

The safer course, if there is any doubt, would be to direct the appropriate state authority to make the application to FTC. The staff recommends that, **if there is a possibility that California law could be considered inconsistent** with GLB, a provision along the following lines should be included in the statute:

> **Preemption**
> (a) Except as provided in this section, this chapter is operative on a determination by the Federal Trade Commission that the chapter is not preempted by the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6807.
> (b) The *state regulatory authority* shall forthwith apply to the Federal Trade Commission for a determination that this chapter is not preempted by the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6807. This subdivision is operative immediately.

Note the final sentence about operative date. We will need to consider deferral issues to allow time for form preparation, etc. See discussion of "Retroactivity and Deferral of Operation" below. But that should not delay steps to obtain a determination of nonpreemption, if need be. One problem is that an urgency clause must be adopted on a two-thirds vote of each house of the Legislature, which may be difficult to achieve in this contentious area.

Suppose California obtains a determination of nonpreemption, but the statute is later amended. Is that determination void, or does it continue in effect until FTC issues a later preemption determination? The federal regulations do not address the issue, and we have no experience in the two states that have received preemption determinations to date. (North Dakota's statute was fundamentally revised by referendum after issuance of the FTC preemption determination, but North Dakota has not reapplied.)

The staff thinks federal law would necessarily preempt an inconsistent state statute until a new FTC determination of "greater protection" is obtained. The staff would **add to the California law a provision that defers the operative date of a revision of the state financial privacy statute that is arguably inconsistent** with GLB until an FTC determination is obtained.

> **Revision of California financial privacy law**
>
> If the *state regulatory authority* determines that there is a likelihood that a revision of this chapter may be inconsistent with the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 USC § 6807:
>
> (a) The *state regulatory authority* shall forthwith apply to the Federal Trade Commission for a determination that the revision is not preempted by that Act.
>
> (b) The revision is operative on a determination by the Federal Trade Commission that the revision is not preempted by that Act.

FCRA Preemption

The Fair Credit Reporting Act regulates communication of information between a credit bureau and third parties bearing on a consumer's credit worthiness, credit standing, credit capacity or other personal information that is used for the purpose of serving as a factor in establishing the consumer's eligibility for credit, insurance, and various other financial purposes. It thus regulates a narrower segment of the financial information spectrum than GLB.

Like GLB, FCRA does not preempt a state statute governing collection, distribution, or use of information about consumers, except to the extent the

statute is "inconsistent" with the act. 15 USC § 1681t(a). However, the act does preempt, until January 1, 2004, state statutes governing exchange of information among affiliates, and various other provisions of the act. After that date a state may enact a statute addressed to those provisions, provided that the statute states explicitly that it is intended to supplement the FCRA and that it gives greater protection to consumers than is provided under the act. 15 USC § 1681t(b), (d).

What would be the effect of the bills pending in Congress to repeal the January 1, 2004, provision? They would preclude the ability of a state to enact a statute that governs exchange of information among affiliates and various other elements of FCRA, whether or not "consistent" with FCRA. For example, no requirement or prohibition could be imposed under the laws of any state with respect to the exchange of information among persons affiliated by common ownership or common corporate control, to the extent FCRA addresses the matter. 15 USC § 1681t(b)(2).

Unlike GLB, FCRA does not look to FTC for a preemption determination. Under FCRA, inconsistent state laws are tested in court. Courts have held, for example:

- Various provisions of a local ordinance, including a requirement that sources of consumer credit report information be disclosed, were held to be inconsistent with FCRA and therefore preempted by it. *Retail Credit Co. v. Dade County, Fla.*, 393 F. Supp. 577 (S.D. Fla. 1975).
- A state law that prohibits a credit bureau from charging a fee for disclosing a credit denial to a consumer is not preempted by the provision of FCRA that allows a credit bureau to charge a reasonable fee. "The philosophy behind both statutes is the protection of the consumer and it is clear that the Federal Act permits Arizona to go further than the Federal Act does to protect consumers as long as the Arizona Act is not inconsistent with the Federal Act." *Credit Data of Ariz. v. State of Ariz.*, 602 F.2d 195, 198 (9th Cir. 1979).
- A state law that requires a customer's separate written consent to a bank's disclosure of insurance information to an affiliated agent or broker was determined by the Office of the Comptroller of the Currency to be preempted by FCRA, and that determination has been upheld. *Cline v. Hawke*, 51 Fed. App. 392 (4th Cir. 2002) (unreported).

Where does all of this leave us? In a quandary, is maybe the best answer.

If the statute enabling more protective state action after January 1, 2004, holds, we can do the same sort of preemption analysis we do under GLB, and make sure that our statute is either (1) consistent with FCRA or (2) if not, that it relates to a matter identified in 15 USC § 1681t(b) or (c) and provides greater protection to consumers.

If the statute enabling more protective state action after January 1, 2004, is repealed, we will need to carve out FCRA coverage from the state privacy law.

At this point the staff doesn't have any good ideas about how best to cover both contingencies. If Congressional action is completed before our study is done, we will know the situation and can shape our recommended legislation accordingly. If not, we will need to maintain some flexibility in the law. One way to do this would be to **put a trigger in the law**, controlled by the state regulatory authority.

> **Fair Credit Reporting Act preemption**
>
> (a) Sections [*here collect the provisions that overlap 15 USC § 1681t(b) and (c)*] do not apply to the collection, distribution, or use of any information on consumers to the extent those activities are subject to the federal Fair Credit Reporting Act, 15 USC § 1681 et seq.
>
> (b) Subdivision (a) is operative on certification pursuant to subdivision (c) that the federal Fair Credit Reporting Act, 15 USC § 1681t(d), has been amended to remove the authority of state law after January 1, 2004, to supplement the Fair Credit Reporting Act and give greater protection to consumers than is provided under that act.
>
> (c) The *state regulatory authority* shall monitor federal legislative action and, if the *state regulatory authority* determines that the federal Fair Credit Reporting Act, 15 USC § 1681t(d), has been amended as provided in subdivision (b), the *state regulatory authority* shall forthwith by regulation certify that subdivision (a) is operative.
>
> **Comment.** This section is triggered only if Congress acts to remove the authority of a state to deal with the matters governed by the Fair Credit Reporting Act that are specified in 15 USC § 1681t(b) and (c). The specific provisions of this chapter that are potentially preempted by those provisions of the Fair Credit Reporting Act are [*here collect and describe the provisions that overlap 15 USC § 1681t(b) and (c)*].

Other Federal Statute Preemption

There are other federal regulatory statutes that arguably could have preemptive effect on state financial privacy laws. The National Bank Act (12 USC § 1), for example, gives the Office of the Comptroller of the Currency broad supervisory jurisdiction over national banks, largely free of state control. Can California regulate financial privacy practices of national banks? This is not a simple question to answer. We have enlisted the Public Law Research Institute of UC Hastings College of Law to analyze the matter. Their work is nearly complete. **We will schedule the matter for discussion** in the near future.

Other federal regulatory statutes govern other types of financial institutions. Each regulatory scheme is unique. We will perform a preemption analysis for each one, as resources permit.

Local Ordinances

The Commission has determined that, at least for purposes of the tentative recommendation circulated for comment, state legislation should preempt local regulation in the field. In order to ensure that this approach is upheld in the courts, the legislation should **include a finding that this is a matter of statewide importance**, rather than a municipal affair, and that local preemption is therefore necessary.

The staff proposes the following draft:

> **Local Preemption**
>
> (a) The Legislature finds and declares that the protection of personal financial information of the citizens of this state is a matter of statewide interest and concern, and that it is in the interest both of the citizens of this state and of entities doing business in this state that uniform statewide standards apply to protection of personal financial information, free of control by local agencies.
>
> (b) This chapter and regulations adopted pursuant to it are of statewide interest and concern and are intended to occupy the field. They preempt and are exclusive of any local agency ordinance, law, or regulation relating to the use and sharing of nonpublic personal information by a financial institution, regardless of whether the local agency ordinance, law, or regulation was adopted before or after the operative date of this chapter.

Contract Clause Issues

The Commission has noted the need for further research on the extent to which state privacy regulations can limit information sharing pursuant to contracts in effect at the time state law is enacted. Staff research on this matter is underway, but we are not yet in a position to make any suggestions concerning it.

Deferred Operative Date

Preemption Determination

GLB does not preempt state law except to the extent state law is inconsistent with GLB. While one would think that more restrictive state privacy regulations would be deemed to be inconsistent with GLB, that is not the case; GLB specifically provides that a state statute is not inconsistent for preemption purposes if the protection it affords any consumer is greater than the protection provided under GLB "as determined by the Federal Trade Commission" after consultation with the relevant federal regulatory authority. The determination may be made by FTC on its own motion or on petition of an interested party. 15 USC § 6807(b); 16 CFR 313.17(b).

Until FTC makes a determination that inconsistent California law provides greater protection than federal law and is therefore not preempted, a financial institution would have a legitimate argument that it is not bound by and need not comply with California law.

How much time should be allowed for a California petition? To date four states have petitioned FTC for a preemption determination. The North Dakota petition took 15 months to determine, the Connecticut petition took 14 months to determine, the Illinois petition has been pending for 22 months and has not yet been determined, and the Vermont petition has been pending for 17 months and has not yet been determined.

One option is to not prescribe an operative date, but to make the statute operative on determination by FTC that the statute is not preempted by federal law. We could expedite the determination by making the statute an urgency measure and directing an appropriate state authority to make the application immediately. However, an urgency statute requires a 2/3 vote, and given the historical difficulty in getting anything enacted on this matter, that large a margin is probably unrealistic.

Would it be possible to obtain some sort of advance ruling on any proposed California statute from FTC? The regulations don't address this matter specifically. Given the workload of FTC and their response time to formal exemption requests, we doubt that a request for a declaratory determination on a Law Revision Commission recommendation would make its way to the top of the in basket.

The staff thinks the better approach is to try to **construct a statute that reasonable minds would agree is not inconsistent with GLB, and make it operative as soon as reasonably possible**, consistent with time required to adopt implementing forms and regulations.

Development of Forms and Issuance of Regulations

The staff has recommended that the state regulatory authority be assigned the task of adopting regulations that detail the application of the law and prescribe the form of the privacy notice. The staff does not anticipate this would consume a lot of time up front — the regulations would be based on federal law, and there are existing examples from which a model form can be derived. However, rulemaking experience under the Administrative Procedure Act suggest that **it would be prudent to provide for six months deferral** of the operative date.

> **Operative date**
>
> (a) Except as provided in subdivision (b), this chapter is operative on July 1, 2006.
>
> (b) The *state regulatory authority* may, on or after January 1, 2006, adopt regulations that implement this chapter.
>
> **Comment.** This section provides a six month deferred operative date to allow for preparation of necessary implementing regulations, including forms. See Sections [*here collect and describe provisions requiring adoption of regulations*].

Severability Clause

Because of the possibility that some aspects of the financial privacy statute will be determined to be federally preempted, **the Commission should consider adding a severability clause**. A severability clause is intended to save independent provisions of a statute that are not affected by preemption. For example, a severability clause could save provisions for consumer control of affiliate sharing even though the details of the privacy notice may be preempted.

Severability Clause

The provisions of this chapter are severable. If a provision of this chapter or its application is held invalid or is preempted by federal law, that invalidity or preemption does not affect any other provision of the chapter or any other application of the provision that can be given effect without the invalid or preempted provision or application.

LOCATION OF CALIFORNIA STATUTE

Where should the California financial privacy statute be located? A logical place would be the Financial Code, and in fact both SB 1 (Speier) and the California Financial Privacy Act ballot initiative would create a new Division 1.2 of the Financial Code (located between Divisions 1.1 (setting fees in consumer credit agreements) and 1.5 (sale, merger, and conversion of depository corporations).

While this location appears appropriate, the staff thinks the Commission should consider other possible locations, given the breadth of coverage of the statute. Granted, the statute relates to "financial" privacy. But it covers not only banks, savings and loan associations, and credit unions, but also securities companies, insurance companies, medical service provides, real estate service providers, retailers who extend credit, and even governmental agencies. Logical places for legislation of this sort, besides the Financial Code, might include the Insurance Code and the Corporations Code, among others.

A superior location, in the staff's opinion, is the Civil Code. That is the locus of a number of existing privacy statutes, and of consumer protections generally. It is a place many different businesses as well as consumers know to look for consumer-related statutes.

One logical location in the Civil Code could be Division 1, Part 2.7 (following Part 2.6 — Confidentiality of Medical Information). A more appropriate location, though, would be among the other Civil Code provisions relating to consumer financial privacy. These are located in Division 3 (obligations) and are clustered in Part 4 (obligations arising from particular transactions) of Division 3:

Part 4. Obligations Arising from Particular Transactions

...

Title 1.8. Personal Data

Chapter 1. Information Practices Act of 1977 (§§ 1798-1798.78)

Title 1.81. Customer Records (§§ 1798.80-1798.84)
Title 1.81.1. Confidentiality of Social Security Numbers (§§ 1798.85-1798.86)
Title 1.81.3. Identity Theft (§§ 1798.92-1798.97)
Title 1.82. Business Records
Chapter 1. Definitions (§ 1799)
Chapter 2. Disclosures (§§ 1799.1-1799.1a)
Chapter 3. Civil Remedies (§§ 1799.2-1799.3)
...

A problem with this location is that it is extraordinarily congested, and a numbering nightmare. While it would be possible to squeeze in the financial privacy statute leaving everything else in place, **maybe this is a good time to consider some statutory reorganization**. We can anticipate, as concern over privacy grows, a dramatic expansion of the law in this area. If the Commission is interested, the staff will investigate this possibility. Factors militating against reorganization include the possible need to correct innumerable cross-references, and the costs of reprinting forms and consumer information to reflect the numbering change.

Meanwhile, the **staff proposes the following location and limited reorganization and renumbering** for the financial privacy statutes (together with conforming revisions to accommodate the reorganization):

Title 1.8. Personal Data
Chapter 1. Information Practices Act of 1977 (§§ 1798-1798.78)
Chapter 2. Financial Privacy (§§ 1798.810-1798.920)
~~Title 1.81~~ Chapter 3. Customer Records (§ ~~1798.80~~ 1798.930)
~~Title 1.81.1~~ Chapter 4. Confidentiality of Social Security Numbers (§ ~~1798.85~~ 1798.940)
~~Title 1.81.3~~ Chapter 5. Identity Theft (§ ~~1798.92~~ 1798.950)
~~Title 1.82~~ Chapter 6. Business Records
~~Chapter~~ Article 1. Definitions (§ ~~1799~~ 1798.961)
~~Chapter~~ Article 2. Disclosures (§ ~~1799.1~~ 1798.963)
~~Chapter~~ Article 3. Civil Remedies (§ ~~1799.2~~ 1798.966)

We might want to consider retitling some of these chapters as well. For example, "Chapter 3. Customer Records" really deals with destruction of records, and "Chapter 6. Business Records" is limited to bookkeeping services. It is also possible that some of these statutes will be eclipsed by the new "Chapter 2. Financial Privacy", and can be repealed. We will not know this until we have completed our work on the matter.

CONFORMING REVISIONS

The Commission has asked the staff to catalog the various existing state privacy statutes, to begin the process of determining whether they overlap the general financial privacy statute. This will be one of the more difficult and time consuming tasks in the project.

Once overlaps have been cataloged, we will need to determine what should be done with them. The basic presumption should be that the general statute does not override a special statute, although the Commission may want to revisit this concept when we have a complete list. In particular, if the general financial privacy statute is more protective of consumer rights than the special statute, that will require careful attention.

Frankly, the staff has not yet had time to begin this process. Perhaps we will have made progress on it by the time of the next Commission meeting.

Respectfully submitted,

Nathaniel Sterling
Executive Secretary

first, (Alternative A) deemed information as publicly available only if a financial institution *actually obtained* the information from a public source, whereas the second (Alternative B) treated information as publicly available if a financial institution *could* obtain it from such a source. A vast majority of commenters favored Alternative B as significantly less burdensome than Alternative A. In response to these comments, the final Rule adopts a modified version of Alternative B, which is more fully explained in the section-by-section analysis.

Content of Notices

Many commenters interpreted the proposed Rule as mandating lengthy, confusing privacy notices that would offer little benefit to consumers, and asked for clarification with respect to the content of those disclosures. Although the Commission believes that the notice obligations are not unduly burdensome, in the final Rule it has taken a number of steps to clarify the requirements imposed by the G-L-B Act. The final Rule substantially revises the examples of disclosures that would satisfy the Rule, includes sample clauses that might be used, and adds a new provision for ''short-form'' privacy notices to a consumer that does not become a customer, provided the institution gives the consumer an opt out notice and a reasonably convenient method of obtaining a copy of the full privacy notice. It also retains the simplified notice provision for institutions that do not share nonpublic personal information with nonaffiliated third parties, except pursuant to the exceptions set forth in §§ 313.14 and 313.15 of this part. These measures may be particularly helpful to smaller institutions who do not disclose nonpublic personal information except under those and other exceptions in the final Rule.

In addition, the Commission has included with the final Rule sample disclosures that institutions may use to draft their privacy and opt out notices required by this part. As discussed in the section-by-section analysis above, these clauses are provided to convey to institutions the requisite level of detail that these notices must contain. Institutions can also consult the Guide for Certain Financial Institutions (''Guide''). The Guide generally clarifies the operation of the final Rule. It also provides an example of a notice for institutions, including small entities, that only share nonpublic personal information with nonaffiliated third parties pursuant to the exceptions provided in §§ 313.14 and 313.15. The Guide may be used in conjunction with the sample clauses contained in Appendix A. Like the examples discussed above, the sample disclosures and the Guide are intended to minimize the burden of complying with the final Rule, by reducing, among other costs, the need for legal advice.

Joint Account Holders

Another frequent comment addressed the provision of notice to and effect of opt outs exercised by joint account holders. As the section-by-section analysis describes, the final Rule clarifies that institutions may provide a single notice to joint account holders (unless otherwise requested), with the understanding that a decision to opt out made by one of the joint account holders will, absent a provision to the contrary in the opt out notice, be effective with respect to each of the account holders. By reducing the number of notices that institutions are required to provide, this flexibility will particularly benefit those institutions, including small entities, that do not share nonpublic personal information with nonaffiliated third parties, except pursuant to an exception.

New Notices Not Required for Each New Financial Product or Service

Some commenters expressed concern that the proposed rule may require a new initial notice each time a consumer obtains a new financial product or service. This would be especially burdensome for an institution that adopts a universal privacy policy that covers multiple products and services. To address these concerns and minimize economic burden, the final Rule was clarified to instruct institutions that a new initial notice is not required if the institution has given the customer the institution's initial notice, and that notice remains accurate with respect to the new product or service.

Section F. Paperwork Reduction Act

Pursuant to the Paperwork Reduction Act, as amended, 44 U.S.C. 3501 *et seq.*, the Commission submitted the proposed Rule to the Office of Management and Budget (OMB) for review. The OMB has approved the Rule's information collection requirements.[42] A **Federal Register** notice with a 30-day comment period of soliciting comments on this collection of information was published on March 1, 2000 (65 FR 11174). The Commission did not receive any comments that necessitated modifying its original burden estimates for the Rule's notice requirements.

Section G. Final Rule

List of Subjects in 16 CFR Part 313

Consumer protection, Credit, Data protection, Privacy, Trade practices.

Accordingly, the Commission amends 16 CFR Ch. I, Subchapter C, by adding a new Part 313 to read as follows:

PART 313—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.

Authority: 15 U.S.C. 6801 *et seq.*

§ 313.1 Purpose and scope.

(a) *Purpose.* This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may

[42] The assigned OMB clearance number is 3084–0121.

disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 313.13, 313.14, and 313.15.

(b) *Scope.* This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to those ''financial institutions'' and ''other persons'' over which the Federal Trade Commission (''Commission'') has enforcement authority pursuant to Section 505(a)(7) of the Gramm-Leach-Bliley Act. An entity is a ''financial institution'' if its business is engaging in a financial activity as described in Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 211.5(d) and 12 CFR 225.28. The ''financial institutions'' subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the Gramm-Leach-Bliley Act. More specifically, those entities include, but are not limited to, mortgage lenders, ''pay day'' lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission. They are referred to in this part as ''You.'' The ''other persons'' to whom this part applies are third parties that are not financial institutions, but that receive nonpublic personal information from financial institutions with whom they are not affiliated. Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d–1320d–8. Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

§ 313.2 Rule of construction.

The examples in this part and the sample clauses in Appendix A of this part are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this part. For non-federally insured credit unions, compliance with an example or use of a sample clause contained in 12 CFR part 716, to the extent applicable, constitutes compliance with this part. For intrastate securities broker-dealers and investment advisors not registered with the Securities and Exchange Commission, compliance with an example or use of a sample clause contained in 17 CFR part 248, to the extent applicable, constitutes compliance with this part.

§ 313.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Affiliate* means any company that controls, is controlled by, or is under common control with another company.

(b)(1) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) *Examples*—(i) *Reasonably understandable.* You make your notice reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible; and

(F) Avoid explanations that are imprecise and readily subject to different interpretations.

(ii) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

(iii) *Notices on web sites.* If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(c) *Collect* means to obtain information that you organize or can retrieve by the name of an individual or by identifying number, symbol, or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e)(1) *Consumer* means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

(2) *Examples*—(i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or

economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(f) *Consumer reporting agency* has the same meaning as in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(g) *Control* of a company means:

(1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

(h) *Customer* means a consumer who has a customer relationship with you.

(i)(1) *Customer relationship* means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) *Examples*—(i) *Continuing relationship.* A consumer has a continuing relationship with you if the consumer:

(A) Has a credit or investment account with you;

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(F) Enters into a lease of personal property on a non-operating basis with you;

(G) Obtains financial, investment, or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a financial institution or department of any company);

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(K) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) *No continuing relationship.* A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a money order from you; cashing a check with you; or making a wire transfer through you;

(B) You sell the consumer's loan and do not retain the rights to service that loan;

(C) You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(j) *Federal functional regulator* means:

(1) The Board of Governors of the Federal Reserve System;

(2) The Office of the Comptroller of the Currency;

(3) The Board of Directors of the Federal Deposit Insurance Corporation;

(4) The Director of the Office of Thrift Supervision;

(5) The National Credit Union Administration Board; and

(6) The Securities and Exchange Commission.

(k)(1) *Financial institution* means any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.

(2) *Examples of financial institution.*

(i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(iii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines,

is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act.

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 211.5(d)(15) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act.

(3) *Financial institution* does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.14 and 313.15 of this part.

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities.

(4) *Examples of entities that are not significantly engaged in financial activities.* (i) A retailer is not a financial institution if its only means of extending credit are occasional ''lay away'' and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to ''run a tab.''

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(l)(1) *Financial product or service* means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) *Financial service* includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(m)(1) *Nonaffiliated third party* means any person except:

(i) Your affiliate; or

(ii) A person employed jointly by you and any company that is not your affiliate (but *nonaffiliated third party* includes the other company that jointly employs the person).

(2) *Nonaffiliated third party* includes any company that is an affiliate by virtue of your or your affiliate's direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

(n)(1) *Nonpublic personal information* means:

(i) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) *Nonpublic personal information* does not include:

(i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) *Examples of lists*—(i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(o)(1) *Personally identifiable financial information* means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples*—(i) *Information included.* Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has

obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet ''cookie'' (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) *Information not included.* Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(p)(1) *Publicly available information* means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) *Reasonable basis.* You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) *Examples*—(i) *Government records.* Publicly available information in government records includes information in government real estate records and security interest filings.

(ii) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) *Reasonable basis*—(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(q) *You* includes each ''financial institution'' (but excludes any ''other person'') over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

Subpart A—Privacy and Opt Out Notices

§ 313.4 Initial privacy notice to consumers required.

(a) *Initial notice requirement.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:

(1) *Customer.* An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 313.14 and 313.15.

(b) *When initial notice to a consumer is not required.* You are not required to provide an initial notice to a consumer under paragraph (a) of this section if:

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 313.14 and 313.15; and

(2) You do not have a customer relationship with the consumer.

(c) *When you establish a customer relationship*—(1) *General rule.* You establish a customer relationship when you and the consumer enter into a continuing relationship.

(2) *Special rule for loans.* You establish a customer relationship with a consumer when you originate a loan to the consumer for personal, family, or household purposes. If you subsequently transfer the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3)(i) *Examples of establishing customer relationship.* You establish a customer relationship when the consumer:

(A) Opens a credit card account with you;

(B) Executes the contract to obtain credit from you or purchase insurance from you;

(C) Agrees to obtain financial, economic, or investment advisory services from you for a fee; or

(D) Becomes your client for the purpose of your providing credit counseling or tax preparation services, or to obtain career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a company or financial institution);

(E) Provides any personally identifiable financial information to you in an effort to obtain a mortgage loan through you;

(F) Executes the lease for personal property with you;

(G) Is an obligor on an account that you purchased from another financial institution and whom you have located and begun attempting to collect amounts owed on the account; or

(H) Provides you with the information necessary for you to compile and provide access to all of the consumer's on-line financial accounts at your Web site.

(ii) *Examples of loan rule.* You establish a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when you:

(A) Originate the loan to the consumer and retain the servicing rights; or

(B) Purchase the servicing rights to the consumer's loan.

(d) *Existing customers.* When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family, or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:

(1) You may provide a revised privacy notice, under § 313.8, that covers the customer's new financial product or service; or

(2) If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

(e) *Exceptions to allow subsequent delivery of notice.* (1) You may provide the initial notice required by paragraph (a)(1) of this section within a reasonable time after you establish a customer relationship if:

(i) Establishing the customer relationship is not at the customer's election; or

(ii) Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.

(2) *Examples of exceptions*—(i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if you acquire a customer's loan, or the servicing rights, from another financial institution and the customer does not have a choice about your acquisition.

(ii) *Substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction when:

(A) You and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service; or

(B) You establish a customer relationship with an individual under a program authorized by Title IV of the Higher Education Act of 1965 (20 U.S.C. 1070 *et seq.*) or similar student loan programs where loan proceeds are disbursed promptly without prior communication between you and the customer.

(iii) *No substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at your office or through other means by which the customer may view the notice, such as through a web site.

(f) *Delivery.* When you are required to deliver an initial privacy notice by this section, you must deliver it according to § 313.9. If you use a short-form initial notice for non-customers according to § 313.6(d), you may deliver your privacy notice according to § 313.6(d)(3).

§ 313.5 Annual privacy notice to customers required.

(a)(1) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. *Annually* means at least once in any period of 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

(2) *Example.* You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

(b)(1) *Termination of customer relationship.* You are not required to provide an annual notice to a former customer.

(2) *Examples.* Your customer becomes a former customer when:

(i) In the case of a closed-end loan, the customer pays the loan in full, you charge off the loan, or you sell the loan without retaining servicing rights;

(ii) In the case of a credit card relationship or other open-end credit relationship, you sell the receivables without retaining servicing rights;

(iii) In the case of credit counseling services, the customer has failed to make required payments under a debt management plan, has been notified that the plan is terminated, and you no longer provide any statements or notices to the customer concerning that relationship;

(iv) In the case of mortgage or vehicle loan brokering services, your customer has obtained a loan through you (and you no longer provide any statements or notices to the customer concerning that relationship), or has ceased using your services for such purposes;

(v) In the case of tax preparation services, you have provided and received payment for the service and no longer provide any statements or notices to the customer concerning that relationship;

(vi) In the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, you have received payment, or you have completed all of your responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.

(vii) In cases where there is no definitive time at which the customer relationship has terminated, you have not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material.

(c) *Special rule for loans.* If you do not have a customer relationship with a consumer under the special rule for loans in § 313.4(c)(2), then you need not provide an annual notice to that consumer under this section.

(d) *Delivery.* When you are required to deliver an annual privacy notice by this section, you must deliver it according to § 313.9.

§ 313.6 Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under §§ 313.4, 313.5, and 313.8 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:

(1) The categories of nonpublic personal information that you collect;

(2) The categories of nonpublic personal information that you disclose;

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under §§ 313.14 and 313.15;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under §§ 313.14 and 313.15;

(5) If you disclose nonpublic personal information to a nonaffiliated third party under § 313.13 (and no exception under §§ 313.14 or 313.15 applies to that disclosure), a separate statement of the categories of information you disclose and the categories of third parties with whom you have contracted;

(6) An explanation of the consumer's right under § 313.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;

(7) Any disclosures that you make under section 603(d)(2)(A)(iii) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that you make under paragraph (b) of this section.

(b) *Description of nonaffiliated third parties subject to exceptions.* If you disclose nonpublic personal information to third parties as authorized under §§ 313.14 and 313.15, you are not required to list those exceptions in the initial or annual privacy notices required by §§ 313.4 and 313.5. When describing the categories with respect to those parties, you are required to state only that you make disclosures to other

nonaffiliated third parties as permitted by law.

(c) *Examples*—(1) *Categories of nonpublic personal information that you collect.* You satisfy the requirement to categorize the nonpublic personal information that you collect if you list the following categories, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with you or your affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer reporting agency.

(2) *Categories of nonpublic personal information you disclose*—(i) You satisfy the requirement to categorize the nonpublic personal information that you disclose if you list the categories described in paragraph (e)(1) of this section, as applicable, and a few examples to illustrate the types of information in each category.

(ii) If you reserve the right to disclose all of the nonpublic personal information about consumers that you collect, you may simply state that fact without describing the categories or examples of the nonpublic personal information you disclose.

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.* You satisfy the requirement to categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information if you list them using the following categories, as applicable, and a few applicable examples to illustrate the significant types of third parties covered in each category.

(i) Financial service providers, followed by illustrative examples such as mortgage bankers, securities broker-dealers, and insurance agents.

(ii) Non-financial companies, followed by illustrative examples such as retailers, magazine publishers, airlines, and direct marketers; and

(iii) Others, followed by examples such as nonprofit organizations.

(4) *Disclosures under exception for service providers and joint marketers.* If you disclose nonpublic personal information under the exception in § 313.13 to a nonaffiliated third party to market products or services that you offer alone or jointly with another financial institution, you satisfy the disclosure requirement of paragraph (a)(5) of this section if you:

(i) List the categories of nonpublic personal information you disclose, using the same categories and examples you used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) State whether the third party is:

(A) A service provider that performs marketing services on your behalf or on behalf of you and another financial institution; or

(B) A financial institution with whom you have a joint marketing agreement.

(5) *Simplified notices.* If you do not disclose, and do not wish to reserve the right to disclose, nonpublic personal information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under §§ 313.14 and 313.15, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(1), (a)(8), (a)(9), and (b) of this section.

(6) *Confidentiality and security.* You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if you do both of the following:

(i) Describe in general terms who is authorized to have access to the information; and

(ii) State whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use.

(d) *Short-form initial notice with opt out notice for non-customers*—(1) You may satisfy the initial notice requirements in §§ 313.4(a)(2), 313.7(b), and 313.7(c) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt out notice as required in § 313.7.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that your privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain that notice.

(3) You must deliver your short-form initial notice according to § 313.9. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to § 313.9.

(4) *Examples of obtaining privacy notice.* You provide a reasonable means by which a consumer may obtain a copy of your privacy notice if you:

(i) Provide a toll-free telephone number that the consumer may call to request the notice; or

(ii) For a consumer who conducts business in person at your office, maintain copies of the notice on hand that you provide to the consumer immediately upon request.

(e) *Future disclosures.* Your notice may include:

(1) Categories of nonpublic personal information that you reserve the right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom you reserve the right in the future to disclose, but to whom you do not currently disclose, nonpublic personal information.

(f) *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this part.

§ 313.7 Form of opt out notice to consumers; opt out methods.

(a) (1) *Form of opt out notice.* If you are required to provide an opt out notice under § 313.10(a), you must provide a clear and conspicuous notice to each of your consumers that accurately explains the right to opt out under that section. The notice must state:

(i) That you disclose or reserve the right to disclose nonpublic personal information about your consumer to a nonaffiliated third party;

(ii) That the consumer has the right to opt out of that disclosure; and

(iii) A reasonable means by which the consumer may exercise the opt out right.

(2) *Examples*—(i) *Adequate opt out notice.* You provide adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if you:

(A) Identify all of the categories of nonpublic personal information that you disclose or reserve the right to disclose, and all of the categories of nonaffiliated third parties to which you disclose the information, as described in § 313.6(a) (2) and (3) and state that the consumer can opt out of the disclosure of that information; and

(B) Identify the financial products or services that the consumer obtains from you, either singly or jointly, to which the opt out direction would apply.

(ii) *Reasonable opt out means.* You provide a reasonable means to exercise an opt out right if you:

(A) Designate check-off boxes in a prominent position on the relevant forms with the opt out notice;

(B) Include a reply form that includes the address to which the form should be mailed; or

(C) Provide an electronic means to opt out, such as a form that can be sent via

electronic mail or a process at your web site, if the consumer agrees to the electronic delivery of information; or

(D) Provide a toll-free telephone number that consumers may call to opt out.

(iii) *Unreasonable opt out means.* You *do not* provide a reasonable means of opting out if:

(A) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(B) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that you provided with the initial notice but did not include with the subsequent notice.

(iv) *Specific opt out means.* You may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

(b) *Same form as initial notice permitted.* You may provide the opt out notice together with or on the same written or electronic form as the initial notice you provide in accordance with § 313.4.

(c) *Initial notice required when opt out notice delivered subsequent to initial notice.* If you provide the opt out notice later than required for the initial notice in accordance with § 313.4, you must also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

(d) *Joint relationships*—(1) If two or more consumers jointly obtain a financial product or service from you, you may provide a single opt out notice, unless one or more of those consumers requests a separate opt out notice. Your opt out notice must explain how you will treat an opt out direction by a joint consumer (as explained in paragraph (d)(5)(ii)of this section).

(2) Any of the joint consumers may exercise the right to opt out. You may either:

(i) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(ii) Permit each joint consumer to opt out separately.

(3) If you permit each joint consumer to opt out separately, you must permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) You may not require *all* joint consumers to opt out before you implement *any* opt out direction.

(5) *Example.* If John and Mary have a joint credit card account with you and arrange for you to send statements to John's address, you may do any of the following, but you must explain in your opt out notice which opt out policy you will follow:

(i) Send a single opt out notice to John's address, but you must accept an opt out direction from either John or Mary.

(ii) Treat an opt out direction by either John or Mary as applying to the entire account. If you do so, and John opts out, you may not require Mary to opt out as well before implementing John's opt out direction.

(iii) Permit John and Mary to make different opt out directions. If you do so,

(A) You must permit John and Mary to opt out for each other;

(B) If both opt out, you must permit both to notify you in a single response (such as on a form or through a telephone call); and

(C) If John opts out and Mary does not, you may only disclose nonpublic personal information about Mary, but not about John and not about John and Mary jointly.

(e) *Time to comply with opt out.* You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive it.

(f) *Continuing right to opt out.* A consumer may exercise the right to opt out at any time.

(g) *Duration of consumer's opt out direction*—(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal information that you collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with you, the opt out direction that applied to the former relationship does not apply to the new relationship.

(h) *Delivery.* When you are required to deliver an opt out notice by this section, you must deliver it according to § 313.9.

§ 313.8 Revised privacy notices.

(a) *General rule.* Except as otherwise authorized in this part, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to that consumer under § 313.4, unless:

(1) You have provided to the consumer a clear and conspicuous revised notice that accurately describes your policies and practices;

(2) You have provided to the consumer a new opt out notice;

(3) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) the consumer does not opt out.

(b) *Examples*—(1) Except as otherwise permitted by §§ 313.13, 313.14, and 313.15, you must provide a revised notice before you:

(i) Disclose a new category of nonpublic personal information to any nonaffiliated third party;

(ii) Disclose nonpublic personal information to a new category of nonaffiliated third party; or

(iii) Disclose nonpublic personal information about a former customer to a nonaffiliated third party if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.

(2) A revised notice is not required if you disclose nonpublic personal information to a new nonaffiliated third party that you adequately described in your prior notice.

(c) *Delivery.* When you are required to deliver a revised privacy notice by this section, you must deliver it according to § 313.9.

§ 313.9 Delivering privacy and opt out notices.

(a) *How to provide notices.* You must provide any privacy notices and opt out notices, including short-form initial notices, that this part requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

(b)(1) *Examples of reasonable expectation of actual notice.* You may reasonably expect that a consumer will receive actual notice if you:

(i) Hand-deliver a printed copy of the notice to the consumer;

(ii) Mail a printed copy of the notice to the last known address of the consumer;

(iii) For the consumer who conducts transactions electronically, clearly and conspicuously post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service;

(iv) For an isolated transaction with the consumer, such as an ATM transaction, post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

(2) *Examples of unreasonable expectation of actual notice.* You may *not,* however, reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:

(i) Only post a sign in your branch or office or generally publish

advertisements of your privacy policies and practices;

(ii) Send the notice via electronic mail to a consumer who does not obtain a financial product or service from you electronically.

(c) *Annual notices only.* You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:

(1) The customer uses your web site to access financial products and services electronically and agrees to receive notices at the web site and you post your current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.

(d) *Oral description of notice insufficient.* You may not provide any notice required by this part solely by orally explaining the notice, either in person or over the telephone.

(e) *Retention or accessibility of notices for customers*—(1) For customers only, you must provide the initial notice required by § 313.4(a)(1), the annual notice required by § 313.5(a), and the revised notice required by § 313.8 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.

(2) *Examples of retention or accessibility.* You provide a privacy notice to the customer so that the customer can retain it or obtain it later if you:

(i) Hand-deliver a printed copy of the notice to the customer;

(ii) Mail a printed copy of the notice to the last known address of the customer; or

(iii) Make your current privacy notice available on a web site (or a link to another web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the web site.

(f) *Joint notice with other financial institutions.* You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions.

(g) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from you, you may satisfy the initial, annual, and revised notice requirements of §§ 313.4(a), 313.5(a), and 313.8(a) by providing one notice to those consumers jointly, unless one or more of those consumers requests separate notices.

Subpart B—Limits on Disclosures

§ 313.10 Limits on disclosure of nonpublic personal information to nonaffiliated third parties.

(a)(1) *Conditions for disclosure.* Except as otherwise authorized in this part, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party unless:

(i) You have provided to the consumer an initial notice as required under § 313.4;

(ii) You have provided to the consumer an opt out notice as required in § 313.7;

(iii) You have given the consumer a reasonable opportunity, before you disclose the information to the nonaffiliated third party, to opt out of the disclosure; and

(iv) The consumer does not opt out.

(2) *Opt out definition.* Opt out means a direction by the consumer that you not disclose nonpublic personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 313.13, 313.14, and 313.15.

(3) *Examples of reasonable opportunity to opt out.* You provide a consumer with a reasonable opportunity to opt out if:

(i) *By mail.* You mail the notices required in paragraph (a)(1) of this section to the consumer and allow the consumer to opt out by mailing a form, calling a toll-free telephone number, or any other reasonable means within 30 days from the date you mailed the notices.

(ii) *By electronic means.* A customer opens an on-line account with you and agrees to receive the notices required in paragraph (a)(1) of this section electronically, and you allow the customer to opt out by any reasonable means within 30 days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(iii) *Isolated transaction with consumer.* For an isolated transaction, such as the purchase of a money order by a consumer, you provide the consumer with a reasonable opportunity to opt out if you provide the notices required in paragraph (a)(1) of this section at the time of the transaction and request that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

(b) *Application of opt out to all consumers and all nonpublic personal information*—(1) You must comply with this section, regardless of whether you and the consumer have established a customer relationship

(2) Unless you comply with this section, you may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer that you have collected, regardless of whether you collected it before or after receiving the direction to opt out from the consumer.

(c) *Partial opt out.* You may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

§ 313.11 Limits on redisclosure and reuse of information.

(a)(1) *Information you receive under an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution under an exception in § 313.14 or 313.15 of this part, your disclosure and use of that information is limited as follows:

(i) You may disclose the information to the affiliates of the financial institution from which you received the information;

(ii) You may disclose the information to your affiliates, but your affiliates may, in turn, disclose and use the information only to the extent that you may disclose and use the information; and

(iii) You may disclose and use the information pursuant to an exception in § 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which you received the information.

(2) *Example.* If you receive a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in § 313.14(a), you may disclose that information under any exception in § 313.14 or 313.15 in the ordinary course of business in order to provide those services. You could also disclose that information in response to a properly authorized subpoena. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

(b)(1) *Information you receive outside of an exception.* If you receive nonpublic personal information from a nonaffiliated financial institution other than under an exception in § 313.14 or 313.15 of this part, you may disclose the information only:

(i) To the affiliates of the financial institution from which you received the information;

(ii) To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and

(iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.

(2) *Example.* If you obtain a customer list from a nonaffiliated financial institution outside of the exceptions in § 313.14 and 313.15:

(i) You may use that list for your own purposes; and

(ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed the list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list, as limited by the opt out direction of each consumer whose nonpublic personal information you intend to disclose, and you may disclose the list in accordance with an exception in § 313.14 or 313.15, such as to your attorneys or accountants.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal information to a nonaffiliated third party under an exception in § 313.14 or 313.15 of this part, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to your affiliates;

(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and

(3) The third party may disclose and use the information pursuant to an exception in § 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

(d) *Information you disclose outside of an exception.* If you disclose nonpublic personal information to a nonaffiliated third party other than under an exception in § 313.14 or 313.15 of this part, the third party may disclose the information only:

(1) To your affiliates;

(2) To its affiliates, but its affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if you made it directly to that person.

§ 313.12 Limits on sharing account number information for marketing purposes.

(a) *General prohibition on disclosure of account numbers.* You must not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

(b) *Exceptions.* Paragraph (a) of this section does not apply if you disclose an account number or similar form of access number or access code:

(1) To your agent or service provider solely in order to perform marketing for your own products or services, as long as the agent or service provider is not authorized to directly initiate charges to the account; or

(2) To a participant in a private label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

(c) *Examples*—(1) *Account number.* An account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code.

(2) *Transaction account.* A transaction account is an account other than a deposit account or a credit card account. A transaction account does not include an account to which third parties cannot initiate charges.

Subpart C—Exceptions

§ 313.13 Exception to opt out requirements for service providers and joint marketing.

(a) *General rule.* (1) The opt out requirements in §§ 313.7 and 313.10 do not apply when you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(i) Provide the initial notice in accordance with § 313.4; and

(ii) Enter into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which you disclosed the information, including use under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out those purposes.

(2) *Example.* If you disclose nonpublic personal information under this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out that joint marketing.

(b) *Service may include joint marketing.* The services a nonaffiliated third party performs for you under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.

(c) *Definition of joint agreement.* For purposes of this section, joint agreement means a written contract pursuant to which you and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service.

§ 313.14 Exceptions to notice and opt out requirements for processing and servicing transactions.

(a) *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 do not apply if you disclose nonpublic personal information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing a financial product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with you, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

(b) *Necessary to effect, administer, or enforce a transaction* means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce your rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(i) To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the consumer's account in the ordinary course of providing the financial service or financial product;

(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(iii) To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;

(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;

(v) To underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or State law;

(vi) In connection with:

(A) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit, or other payment card, check, or account number, or by other payment means;

(B) The transfer of receivables, accounts, or interests therein; or

(C) The audit of debit, credit, or other payment information.

§ 313.15 Other exceptions to notice and opt out requirements.

(a) *Exceptions to opt out requirements.* The requirements for initial notice in § 313.4(a)(2), for the opt out in §§ 313.7 and 313.10, and for service providers and joint marketing in § 313.13 do not apply when you disclose nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2)(i) To protect the confidentiality or security of your records pertaining to the consumer, service, product, or transaction;

(ii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(iii) For required institutional risk control or for resolving consumer disputes or inquiries;

(iv) To persons holding a legal or beneficial interest relating to the consumer; or

(v) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants, and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 *et seq.*), to law enforcement agencies (including a federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a State insurance authority, with respect to any person domiciled in that insurance authority's State that is engaged in providing insurance, and the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

(5)(i) To a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), or

(ii) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or

(7)(i) To comply with Federal, State, or local laws, rules and other applicable legal requirements;

(ii) To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, State, or local authorities; or

(iii) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance, or other purposes as authorized by law.

(b) *Examples of consent and revocation of consent.* (1) A consumer may specifically consent to your disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to you for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under § 313.7(f).

Subpart D—Relation to Other Laws; Effective Date

§ 313.16 Protection of Fair Credit Reporting Act.

Nothing in this part shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), and no inference shall be drawn on the basis of the provisions of this part regarding whether information is transaction or experience information under section 603 of that Act.

§ 313.17 Relation to State laws.

(a) *In general.* This part shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such State statute, regulation, order, or interpretation is inconsistent with the provisions of this part, and then only to the extent of the inconsistency.

(b) *Greater protection under State law.* For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this part if the protection such statute, regulation, order, or interpretation affords any consumer is greater than the protection provided under this part, as determined by the Commission on its own motion or upon the petition of any interested party, after consultation with the applicable federal functional regulator or other authority.

§ 313.18 Effective date; transition rule.

(a) *Effective date.* (1) *General rule.* This part is effective November 13, 2000. In order to provide sufficient time for you to establish policies and systems to comply with the requirements of this part, the Commission has extended the time for compliance with this part until July 1, 2001.

(2) *Exception.* This part is not effective as to any institution that is significantly engaged in activities that the Federal Reserve Board determines, after November 12, 1999, (pursuant to its authority in Section 4(k)(1–3) of the Bank Holding Company Act), are activities that a financial holding company may engage in, until the Commission so determines.

(b)(1) *Notice requirement for consumers who are your customers on the compliance date.* By July 1, 2001, you must have provided an initial notice, as required by § 313.4, to consumers who are your customers on July 1, 2001.

(2) *Example.* You provide an initial notice to consumers who are your customers on July 1, 2001, if, by that

date, you have established a system for providing an initial notice to all new customers and have mailed the initial notice to all your existing customers.

(c) *Two-year grandfathering of service agreements.* Until July 1, 2002, a contract that you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of § 313.13(a)(1) of this part, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as you entered into the contract on or before July 1, 2000.

Appendix A to Part 313—Sample Clauses

Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets and income, and information from a consumer reporting agency, may give rise to obligations under the Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A–1—Categories of Information You Collect (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(1) to describe the categories of nonpublic personal information you collect.

Sample Clause A–1

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates, or others; and
- Information we receive from a consumer reporting agency.

A–2—Categories of Information You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use one of these clauses, as applicable, to meet the requirement of § 313.6(a)(2) to describe the categories of nonpublic personal information you disclose. You may use these clauses if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–2, Alternative 1

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–2, Alternative 2

We may disclose all of the information that we collect, as described [*describe location in the notice, such as ''above'' or ''below''*].

A–3—Categories of Information You Disclose and Parties to Whom You Disclose (Institutions That Do Not Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirements of §§ 313.6(a)(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose. You may use this clause if you do not disclose nonpublic personal information to any party, other than as permitted by the exceptions in §§ 313.14, and 313.15.

Sample Clause A–3

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A–4—Categories of Parties to Whom You Disclose (Institutions That Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15, as well as when permitted by the exceptions in §§ 313.14, and 313.15.

Sample Clause A–4

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [*provide illustrative examples, such as ''mortgage bankers, securities broker-dealers, and insurance agents''*];
- Non-financial companies, such as [*provide illustrative examples, such as ''retailers, direct marketers, airlines, and publishers''*]; and
- Others, such as [*provide illustrative examples, such as ''non-profit organizations''*].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A–5—Service Provider/Joint Marketing Exception

You may use one of these clauses, as applicable, to meet the requirements of § 313.6(a)(5) related to the exception for service providers and joint marketers in § 313.13. If you disclose nonpublic personal information under this exception, you must describe the categories of nonpublic personal information you disclose and the categories of third parties with whom you have contracted.

Sample Clause A–5, Alternative 1

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [*provide illustrative examples, such as ''your name, address, social security number, assets, and income''*];
- Information about your transactions with us, our affiliates, or others, such as [*provide illustrative examples, such as ''your account balance, payment history, parties to transactions, and credit card usage''*]; and
- Information we receive from a consumer reporting agency, such as [*provide illustrative examples, such as ''your creditworthiness and credit history''*].

Sample Clause A–5, Alternative 2

We may disclose all of the information we collect, as described [*describe location in the notice, such as ''above'' or ''below''*] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A–6—Explanation of Opt Out Right (Institutions that Disclose Outside of the Exceptions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(6) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. You may use this clause if you disclose nonpublic personal information other than as permitted by the exceptions in §§ 313.13, 313.14, and 313.15.

Sample Clause A–6

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [*describe a reasonable means of opting out, such as ''call the following toll-free number: (insert number)''*].

A–7—Confidentiality and Security (All Institutions)

You may use this clause, as applicable, to meet the requirement of § 313.6(a)(8) to describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A–7

We restrict access to nonpublic personal information about you to [*provide an appropriate description, such as ''those employees who need to know that information to provide products or services to you''*]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

By direction of the Commission.

Approved by the Commission on May 12, 2000.

Donald S. Clark,

Secretary.

[FR Doc. 00–12755 Filed 5–23–00; 8:45 am]

BILLING CODE 6750–01–P

Personal Insurance Federation of California

California's Personal Lines Trade Association
REPRESENTING THE LEADING AUTOMOBILE AND HOMEOWNERS INSURERS
Progressive • State Farm • Farmers • 21st Century Insurance Group • SAFECO

February 10, 2003

Law Revision Commission
RECEIVED
FEB 11 2003
File:

Nathaniel Sterling, Executive Secretary
California Law Revision Commission
4000 Middlefield Road, Room D-1
Palo Alto, California
94353-4739

Re: ACR 125; Financial Privacy Study

Dear Mr. Sterling:

Thank you for the opportunity to comment at the California Law Revision Commission public hearing held on February 7th. In my comments, I mentioned that insurance companies are often organized as groups of affiliated companies for regulatory, legal, and solvency purposes. I also stated that in some cases companies have indicated that they are organized that way because they have been required by law to offer different lines of insurance through separate companies. You asked us to provide additional information on the applicable laws that might necessitate that insurers organize as affiliates or separate subsidiary companies. We have researched this issue further and hope that the following information is helpful in more clearly explaining this issue.

The legal rules and business practices surrounding insurer organizational structures are complex, and I do not pretend to be an expert in this area of corporate law. Consequently, I will provide a brief overview, but can seek additional analysis from corporate counsel specializing in insurer company organization if further details are desired.

Based on my research, it appears that while insurers originally organized as groups of affiliated companies due to state regulatory requirements, these continued structures today are in many cases the result of historical rather than current regulatory requirements. Historically, the business of insurance developed along different lines of insurance that corresponded to the various kinds of risks being covered. Insurance companies tended to specialize in one line, and sometimes government regulations prevented them from writing in a different line of insurance. As a result, the business of insurance became compartmentalized according to the kind of risk insured. Simultaneously, principles of law evolved for each of these different lines, which institutionalized a number of demarcations that persist in the substantive law of insurance to this day.[1]

Early statutory regulation of the insurance business as well as insurer specialization in particular lines resulted in the recognition of three major

[1] Understanding Insurance Law, Robert H. Jerry II and Matthew Bender, p. 22

980 NINTH STREET • SUITE 2030 • SACRAMENTO, [illegible] PHONE (916) 442 • 6646 • FAX (916) 446 • 9548
E-MAIL: info@pifc.org • WEBSITE: www.pifc.org

categories of insurance: marine and inland marine, life, and fire & casualty. Statutes in many states confined insurers to writing insurance in only one line. Over time, however, many of these restrictions were removed, and some insurers commenced what was called "multiple line" underwriting. This was often done through an affiliated group of insurance companies, each specializing in a particular line. Even in those states which did not allow a single company to engage in multiple-line underwriting, many insurers developed an equivalent to multiple-line underwriting by arranging for the affiliation of several insurance companies whose common agents could provide an insured with a single policy that included several different classes of coverages, each of which was written by one of the affiliated companies. Generally, this marketing arrangement involved a parent company and a group of subsidiaries.[2] This organizational structure is still common today, and describes many insurance company organizational structures.

Separate categories of insurance, classified according to risk, are still preserved in the statutory and common law principles that apply uniquely to each category. Consequently, many companies are organized as affiliated groups today for practical reasons, since particular underwriting, rating, and capitalization requirements apply to each line.

The California Insurance Code, Section 100, today distinguishes the following classes of insurance: life, fire, marine, title, surety, disability, plate glass, liability, workers compensation, common carrier liability, boiler and machinery, burglary, credit, sprinkler, team and vehicle, automobile, mortgage, aircraft, mortgage guaranty, insolvency, legal insurance, and miscellaneous. However, for insurance company licensure requirements, the code groups all these classes together, with the exception of life, title, mortgage, and mortgage guaranty insurance. Thus, it would appear that fire & casualty products and life insurance cannot be sold under the same company license or certificate of authority, but require a separate license.

Reserves/Policyholder Protection/Solvency Requirements

Each insurer is required to maintain reserve funds that consist of an amount reserved from premium to enable the insurer to meet the obligations that it must pay out in any given year. Reserve fund requirements are based on the overall risks assumed by the company and anticipated or predicted liabilities. If the assets of the insurer fall below the amount necessary to maintain the reserve fund, plus any other liabilities, the laws of most states empower the Insurance Commissioner to take control of the company and dissolve it for the benefit of creditors.

As a precaution against allowing assets to fall below the amount necessary to maintain its reserve, insurers also set aside out of income an additional fund called the "surplus fund" or "contingency fund" as a precaution in the event losses far exceed those predicted. This allows an insurer to weather a massive disaster without risking insolvency. (See Section 700.01 regarding paid-in capital requirements for insurers' admitted into one or more classes of insurance, Section 700.02 requiring insurers to have a surplus of at least 100% of required minimum paid-in capital requirements, 706.5 authorizing commissioner to deny a certificate of authority or prohibit the writing of new business if sufficient company investments are not liquid, and Section 739 et seq regarding risk-based capital requirements.)

One of the key reasons why an insurer might sell different insurance products or classes of insurance through separate affiliates is to protect the assets and policyholders of the other

[2] Insurance Law: A Guide to Fundamental Principles, Legal Doctrines, and Commercial Practices, Robert Keeton and Alan I. Widiss, West Group, p. 18

affiliates, should a disaster occur. For instance, in the case of a major earthquake that could bankrupt an insurer's homeowners or earthquake insurance company, the insurer protects the assets and interests of the policyholders of the auto company, by segregating these lines into separate affiliated companies. This is also a key reason why companies sometimes set up separate stand-alone affiliates in certain states, such as California, Florida and Texas. In that way, policyholders in all 50 states are not put at risk by earthquakes in California, hurricanes in Florida, and tornadoes and hail in Texas.

Holding Company Act

The Insurance Holding Company System Regulatory Act governs insurer affiliate/subsidiary relationships. One of the purposes behind the holding company laws is to prevent companies from shifting assets around to avoid capitalization or taxation requirements. The law does not require that insurers be organized as affiliated companies, but strictly regulates such arrangements. The Act, which is found at Insurance Code Section 1215 et seq, defines an affiliate as one controlled by or under common control with another. The Act defines a subsidiary of an entity as an affiliated company controlled by that parent entity. The Act regulates allowed investments, policyholder surplus requirements, securities, and registration requirements. Insurers are required to report to the Insurance Commissioner on capital structure, financial condition, and agreements between an insurer and its affiliates, including loans, extensions of credit, investments, securities exchanges, management agreements, dividends, and tax agreements.

Types of Insurers

Insurers in California may be incorporated as stock companies, mutual companies (which are owned by the policyholders), or reciprocals. Special statutory rules apply to each of these types of companies. Section 1280 et seq governs reciprocals and inter insurance exchanges, a unique type of insurer group structure which also includes affiliates. These governing sections are complex and detailed.

Insurers also organize as groups of affiliated companies for other reasons, including state and federal taxation laws, liability laws, and for reasons related to the particular regulatory rules of a given state. Insurers might also be organized as affiliates for reasons related to the company's own unique business plan.

I hope this letter is responsive to your request. Please let me know if we can provide any additional information that would be useful for your study.

Sincerely,

G. Diane Colborn

G. Diane Colborn

cc: Dan Dunmoyer

FSPC
Financial Services Privacy Coalition

To: California State Senate
From: Financial Services Privacy Coalition
Re: SB 1 (Speier) Oppose Unless Amended
Date: February 28, 2003

The Financial Services Privacy Coalition, an organization of financial institutions and trade associations interested in issues of financial privacy, respectfully opposes SB 1 (Speier). This letter is intended to illuminate only the highest priority concerns shared by all of our members. Individual FSPC members have a variety of specific objections. If the Legislature hopes to enact a workable and fair privacy bill this year, it must address both these concerns and the many concerns that FSPC members will be raising separately.

Introduction. SB 1 is far broader than is needed to address any identified problem. Any unnecessary regulation of information exchange will impose needless costs upon businesses. In a variety of ways, SB 1 takes a costly approach where a more focused approach would produce the same outcome far more efficiently. If the Legislature hopes to enact a workable bill, cost implications must be considered in developing the proposal. In a time when many businesses view California as a "business-unfriendly" state, imposition of legislation that is needlessly costly should be particularly avoided.

Regulation of Information Sharing for Marketing Purposes. Information is used for one of three purposes: transactions, operations or marketing. SB 1 attempts to cover every exchange of information by a regulated business. Each exchange of information must be put into one of three categories: those that are permitted by a specific exemption, those that require opt-out permission, and those that require opt-in permission. This approach is costly and imposes unnecessary legal and regulatory burdens upon covered businesses. It will disrupt customer service.

Proponents of increased regulation generally agree that transactional and operational uses of information should be excluded from the bill. Their primary concern is with the sharing of customer information with a third party so that third party can market its products or services to that customer (the exchange of information for marketing purposes). This issue can be addressed more directly and cost-effectively if the bill regulates only the exchange of information for marketing purposes.

Although SB 1 contains a large number of "transactional" and "operational" exemptions, these do not solve the problem. The list of transactional exemptions in SB 1 is limited to the exchanges of information envisioned by the drafters at this time. This eliminates innovation and freezes product development at current market practices.

Also, the regulate-everything approach means that *every* information exchange must be evaluated in terms of the applicability of the exemptions. The results are not always clear. For example, the most broadly-applicable exemption is for exchanges "necessary to effect, administer, or enforce" a transaction. Reliance upon this "exemption" will require businesses, and their lawyers, to evaluate *every* type of information exchange within each family of affiliated businesses – even the most innocuous – and ask "is this exchange absolutely "necessary?" Even if an exchange is deemed to be necessary, the burden of making this practical and legal evaluation is staggering. Furthermore, there will be many cases in which a business will believe that an exchange is necessary and an attorney will disagree. These cases will result in exhaustive litigation. Lawyers will benefit, but consumers will not.

Because SB 1 regulates *all* information exchange, this ambiguity will be repeated with respect to literally millions of routine and reasonable information exchanges. The bill should be limited to regulating exchanges of information *for marketing purposes* in order to avoid this problem and create a workable and cost-effective bill.

Choosing Marketplace Winners and Loses. SB 1 regulates all exchanges of information within a single organization made up of separate affiliated entities. In some cases the rules for affiliates would differ from the rules applicable to direct competitors providing services under contracts. This results in a law that chooses winners and losers in the marketplace. Although one of the stated purposes of the bill is "to provide a level playing field among types and sizes of businesses," its regulatory approach creates an inevitable obstacle to achieving that purpose.

The fundamental problem is that instead of focusing on the confidentiality and protection of information, SB 1 regulates based upon business structure. This ignores market reality. A single business may organize as two or more affiliated entities for a variety of reasons unrelated to information exchange. Two businesses that are direct competitors in the marketplace, providing identical products and services to consumers, will be regulated differently under SB 1 if one is a single entity with different departments and the other uses separate legal affiliates to provide the identical competitive services. This not only applies to financial institutions but to non-financial institutions as well. For example, a retailer that has an affiliated bank is subject to an opt-out standard while a retailer that contracts with a financial institution to provide credit services is subject to an opt-in standard. Although the customer information is protected equally, the law discriminates between businesses based on their structure. This inequity must be eliminated.

There are many different legal structures, all of which would fall under the general definition of "affiliates" in SB 1. For some of these structures, SB 1 would not involve significant changes in their operations. For others it will be costly and disruptive. In order to create a workable and cost-effective bill, the Legislature must give serious consideration to this issue and address it in a manner that maintains parity between businesses with affiliates and businesses that must use third party financial institutions to deliver products and services to their customers (joint marketing agreements).

Notice Requirements. SB 1 requires a separate defined notice to be given to California customers. The notice would be a specific mandated form unique to California and may not be combined with other privacy notices required by federal and state law. This is unnecessarily costly, unworkable, and does not serve consumers well. Requiring duplicative and inconsistent privacy notices under different provisions of federal and state law would simply confuse California consumers. Insurance customers would be particularly confused since the California Insurance Code already requires an annual privacy notice – a fact that is ignored by SB 1.

There should be no defined "opt-in" form. If opt-in permission is required, the burden is upon the business to be able to document that a real, knowing permission was made by the consumer. If a business attempted to exchange information requiring opt-in permission without clearly obtaining such knowing permission, it would be subject to serious legal liability under existing laws. There is no public policy rationale for defining a particular opt-in form.

Opt-out forms should be based upon statutory standards – in the way that notices are now defined for insurers – not upon a one-size-fits-all mandatory template. They should, for workability reasons, be combinable with other mandated privacy forms, so that consumers do not receive duplicate inconsistent forms. If there is to be an opt-out form offered in statute, it should be done on a "safe-harbor" basis under which use of the form document creates an absolute presumption of complying with the law, but under which a financial institution could also use functionally equivalent forms that meet the standards of the law.

Conclusion. Again, this letter does not provide an exhaustive list of FSPC concerns with SB 1. These concerns reflect only the most serious obstacles to creating a fair and workable privacy law. Many implementation and workability problems also remain. For example, we believe that consideration should be given to making the opt-in requirement prospective only to avoid disruption of services that consumers favor and have become used to. The Legislature should also look at appropriate effective dates for the various provisions of the bill and deal with many technical and drafting problems that remain in the bill. We are at the beginning of the current legislative session and anticipate that additional work will occur on SB 1. We urge the Legislature to address the issues outlined above as this work proceeds.

Aegon Insurance
American Insurance Association
Association of California Life and Health Insurance Companies
Bank of America
California Bankers Association
California Chamber of Commerce
Capital One
Citicorp
Countrywide Mortgage
Farmers Insurance
JP Morgan Chase
MBNA
Providian
Securities Industry Association
State Farm Insurance
USAA Group
Washington Mutual
Wells Fargo

SA2003RF0006, Amdt #2-NS

PROPOSED LAW

SECTION 1. The People of the State of California find and declare:

(a) Banks, insurance companies and other financial institutions invade our privacy when they sell or share our personal information without our permission.

(b) California consumers deserve real control over the sharing of personal information about us and our families by financial institutions.

(c) The more easily our personal information is shared by financial institutions, the more likely it is that our information will be misused or stolen, increasing the possibility of identity theft and other types of fraud.

(d) Current laws are too weak and do not give California consumers enough control over the selling or sharing of our personal information by financial institutions.

(e) The purpose of the California Financial Privacy Act of 2004 is to give consumers control over the sharing of their personal information by financial institutions.

(f) Financial institutions should have the ability to share the minimum amount of Confidential Consumer Information necessary to process transactions requested by consumers and for such other appropriate purposes as preventing fraud or for regulatory or law enforcement purposes, subject to the protections of this act.

SEC. 2. Division 1.2 (commencing with Section 4050) is added to the Financial Code to read:

DIVISION 1.2 CALIFORNIA FINANCIAL PRIVACY ACT

4050. This division shall be known and may be cited as the California Financial Privacy Act.

4051. (a) A financial institution shall not disclose a California consumer's Confidential Consumer Information to another person or entity, including an affiliate, unless the financial institution has obtained, and maintains a record of, the express, affirmative consent of the consumer, or except as provided in this division.

(b) Such express consent may only be obtained by means that provide clear, conspicuous and accurate notice to the consumer of the consumer's financial privacy rights under this section, the nature of the consent sought and the effect of giving such consent. The Attorney General shall issue regulations no later than six months after passage of this division regarding the means by which financial institutions obtain consent.

(c) A consumer shall have the right to modify or revoke such consent at any time.

(d) A financial institution shall not condition or deny a financial product or service to a California consumer because the consumer has not provided or has revoked consent for the disclosure of his or her Confidential Consumer Information under this section.

4052. This division shall not prohibit the disclosure of Confidential Consumer Information which is expressly permitted by Section 502(e) of the federal Gramm-Leach-Bliley Financial Modernization Act and regulations promulgated pursuant thereto in effect on January 1, 2002, such as processing or enforcing transactions requested by the consumer, detecting or preventing fraud and for regulatory or law enforcement purposes. A person or entity that receives Confidential Consumer Information from a financial institution pursuant to this section shall not, directly or indirectly, disclose such information to any other person or entity except as allowed by this division.

4053. "Confidential Consumer Information" means any information pertaining to a California consumer that: (1) the consumer provides to a financial institution to obtain a financial product or service, (2) results from any transaction involving a financial product or service between the financial institution and the consumer, or (3) the financial institution otherwise obtains in connection with providing a financial product or service to the consumer. Confidential Consumer Information includes any list, description, or other grouping of consumers (and any publicly available information pertaining to them) that is derived using any Confidential Consumer Information. "California consumer" means an individual resident of this state, whose last known mailing address, as shown in the records of the financial institution, is located in California. The other terms used herein shall have the same meaning as in the federal Gramm-Leach-Bliley Financial Modernization Act and its implementing regulations in effect on January 1, 2002.

4054. If a violation of this division results in identity theft as defined in Section 530.5 of the California Penal Code, any civil penalties for such violations of this division shall be doubled.

4055. This division shall become operative ten months after passage.

SEC. 3. This act may be amended by a bill approved by a majority vote of the membership of each house of the Legislature and signed by the Governor. All amendments to this act must be to further the act and must be consistent with its purpose which is to maximize the privacy of California consumers by ensuring their Confidential Consumer Information is not disclosed unless the consumer has expressly, affirmatively consented to such disclosure, or except as provided in Section 4052.

SEC. 4. The provisions of this act shall be severable, and if any phrase, clause, sentence, or provision is declared to be invalid or unenforceable for any reason, including preemption by federal law or regulation, the validity of the remainder of this division shall not be affected thereby and shall remain in effect.