Study B-400 January 17, 2003

Memorandum 2003-1

Financial Privacy: Overview

INTRODUCTION

This memorandum inaugurates the Commission's study of financial privacy. The study was directed by the Legislature in 2002. See 2002 Cal. Stat. res. ch. 167, attached at Exhibit p. 1. Under the legislative resolution, the Commission's report and recommended legislation on the matter are due by January 1, 2005.

This memorandum introduces the topic and surveys some of the major legal issues that will need to be resolved. Attached as an Exhibit are copies of or citations to several key legal documents. These documents will provide a useful reference point throughout the project.

Please bear in mind that the topic of financial privacy is large, and expanding rapidly. In addition to both state and federal statutes on the matter, the body of implementing regulations, administrative rulings, and judicial decisions is mounting. An introductory memorandum of this sort can only provide a snapshot and overview. We will get into specific issues in depth as the study progresses.

The purpose of this memorandum is to initiate the Commission's consideration by giving some context to the discussion. While the memorandum does not purport to be a comprehensive dissertation, it is intended to help focus the debate and to act as a stimulus for discussion of issues.

OUTLINE OF MEMORANDUM

COMMISSION STUDY

A typical Commission study begins with an overview and survey of possible directions. After receiving input from interested persons, the Commission makes policy decisions as to the direction the law should take. That is followed by consideration of specific issues and drafting of implementing legislation. Out of this process emerges a tentative recommendation, which the Commission circulates widely for comment. The Commission reviews the comments and makes any necessary revisions before submitting a final recommendation to the Governor and Legislature.

We are at the initial phase of this project. The Commission should take this opportunity to receive input from interested persons as to general perspectives, before focusing on policy decisions and specific statutory language.

To some extent, the public policy parameters of this study have been set for us by the Legislature in the resolution directing the study. The Legislature has made clear that there is a strong public policy in favor of financial privacy:

> The citizens of California have indicated their great concern with this issue, and have made clear their overwhelming desire to have control over the disclosure of their nonpublic personal information.

2002 Cal. Stat. res. ch. 167.

To implement this public policy, the Legislature is looking to the Commission for proposals that will do all of the following:

(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 or 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.

BACKGROUND

Growth of Privacy Concerns

It will be useful to place the concern about financial privacy in context. That concern has grown over the years as problems and abuses have come to light. Some of the significant factors contributing to the current concern include the vulnerability of personal financial information to fraud and identity theft, overly aggressive marketing techniques, and the potential of computerization and electronic data transmission to magnify these problems.

It is not our purpose here to chronicle the rise of financial fraud and identity theft, in all its varieties. Obviously, financial crimes have always existed in various forms, including forgery, embezzlement, and the like. But the increased use of credit and debit cards, automatic teller machines, telephonic and on-line contracting, and other fixtures of contemporary consumer financial transactions, has made consumer financial information more accessible to third parties, with predictable results.

Apart from fraudulent appropriation of personal financial information, a financial institution may use, or transmit for use by others, information properly acquired for an unrelated purpose. For example, a consumer may provide a financial institution sensitive identifying information on a loan or credit card

application, such as address, phone number, social security number, and mother's maiden name. Other data maintained by a financial institution may include account balance, payment and overdraft history, debit and credit card purchases, and insurance coverage (including medical insurance and claim history). The financial institution may take advantage of its possession of this information to target and market other financial, or nonfinancial, products to the consumer. The financial institution may transmit this information to third parties, which in turn may use it for their own purposes.

The explosion of telemarketing calls to consumers at their homes at dinnertime is symptomatic of the increased use of personal financial information for marketing purposes. In fact, it is this sort of annoyance, in addition to the concern about identity theft and invasion of privacy generally, that has fueled efforts to protect financial privacy.

Not all telemarketing techniques have been as benign as a phone call making an attractive offer to the consumer. In 1999, a Minnesota Attorney General's investigation revealed that major national banks had been sharing customer data with direct marketing firms whose aggressive sales tactics included a direct deduction from the customer's account without express authorization. This technique — known as "pre-acquired account telemarketing" — is used to bill the consumer's account if the consumer expresses an interest in the product. It has been reported that during a 13-month period, one bank had to cancel 173,543 membership clubs and insurance policies charged to the accounts of customers who had not authorized and did not want the purchase. The scandal was the trigger for the privacy protections built into the federal Gramm-Leach-Bliley Act.

Sale of customer demographic information is not new. Businesses have long sold customer lists to advertisers. But the size of the business has grown as technology has made it easier to electronically search, gather, and transmit large amounts of data electronically. Customer lists are valuable property. Sale of lists is now a major financial service industry.

Computerization and electronic communications offer unprecedented opportunities for dissemination and misuse of consumer financial information. They have also fueled widespread public concern about erosion of privacy generally, not just with respect to financial information. The legislative response to privacy concerns must be viewed in this context.

Legislative Action

On the first day of California's 2003 legislative session (December 2, 2002), half a dozen bills directed to privacy issues generally, and financial privacy specifically, were introduced. These included:

- AB 7 (Corbett) – Legislature intends to adequately and fully protect privacy rights
- SB 1 (Speier) – California Financial Information Privacy Act
- SB 25 (Bowen) – credit report security alert
- SB 27 (Figueroa) – personal information transferred to a third party for direct marketing purposes
- SJR 1 (Figueroa) – memorializes Congress not to preempt state privacy laws, particularly by the Fair Credit Reporting Act

The California Legislature has enacted several dozen major privacy bills over the past several years, including creation of the state Office of Privacy Protection. (That office maintains an excellent website on privacy protection. The URL is www.privacy.ca.gov.) A listing of the major California privacy statutes, as well as the major federal statutes, is attached to this memorandum at Exhibit p. 3. The listing is printed from Office of Privacy Protection web site.

Gramm-Leach-Bliley Act

In November 1999, Congress enacted the Financial Services Modernization Act, commonly known as the Gramm-Leach-Bliley Act ("GLB"). This statute overturned depression-era and later laws that had erected legal barriers between commercial banking, securities, and insurance industries. GLB repealed essential elements of both the Glass-Steagall Act (which had prevented banks from affiliating with securities companies), and the Bank Holding Company Act (which had blocked a bank from controlling a nonbank company and from conducting insurance activities). Now for the first time since the depression, a financial institution may engage in banking, insurance, and securities businesses simultaneously.

The intention of GLB was to benefit consumers by enhancing competition in domestic financial services. It also was intended to strengthen the ability of domestic companies to compete internationally. In effect, it allows the creation of financial supermarkets by means of financial holding companies created by merger of different types of financial service entities.

The possibility of such a concentration of financial power carries with it unprecedented threats to privacy. Congress dealt with the privacy concern by including in GLB limitations on the extent to which a financial institution may transfer to third parties personal financial information that it has collected concerning its customers. The text of Title V of GLB (15 USC §§ 6801-6810) — "Disclosure of Nonpublic Personal Information" — is set out at Exhibit p. 5.

GLB requires a financial institution annually to send a notice to its customers describing its privacy policy and any nonpublic personal information it intends to disclose to affiliates or third parties. The law also requires a financial institution to provide a method for its customers to prevent, or "opt out" of, the disclosure of some types of information to some types of third parties in some circumstances. GLB also requires a financial institution to develop policies to promote data security. And it creates a right of enforcement — not in individuals but in a number of federal agencies, including the Federal Trade Commission, the Board of Governors of the Federal Reserve System, the Comptroller of Currency, and Securities and Exchange Commission. GLB also allows the states to provide greater privacy protections for consumers.

In May 2000, the Federal Trade Commission ("FTC") issued its implementing regulations. See 16 CFR 313. The other federal enforcement agencies issued parallel regulations. For simplicity, in this memorandum, we refer only to the FTC regulations and not to the parallel agency regulations.

We will get into the details of GLB and implementing regulations later in this memorandum and during the course of this study. Suffice it for now to say that neither financial institutions nor consumers are particularly enthralled with the personal information disclosure aspects of the law in its present form.

In brief, the financial services industry takes the position that it is wasteful for it to send out annual privacy notices to customers. The great majority of their customers just throw the notices away without reading them. Of those who actually read the notices, only a few choose to opt out of sharing information. The cost of this exercise is ultimately expressed in an increase in the price of financial services for all customers. Moreover, easy sharing of financial information is actually in the consumer's best interest because it facilitates financial transactions and makes available to the consumer targeted marketing opportunities of which the consumer might not otherwise be aware.

Consumer advocates argue that few people read the privacy notices or exercise their rights because the notices are issued in fine print legalese, designed

to discourage the recipients from exercising their opt out rights. Moreover, even if a customer elects to opt out, GLB limits the scope of the opt out. Under GLB, a customer cannot preclude the financial institution from sharing the customer's personal information with an "affiliate" of the financial institution, or with a third party with which the financial institution has a "joint marketing agreement". Consumers argue that the state should take advantage of the right provided by GLB to enact better privacy protections than the minimal provisions of GLB.

These concerns are expressed in the resolution that authorized the present study:

> WHEREAS, The Financial Services Modernization Act, commonly know as the Gramm-Leach-Bliley Act, became law in 1999, and reformed the laws that define and regulate the structure of the financial services industry; and
>
> WHEREAS, The Gramm-Leach-Bliley Act greatly liberalized the ways that financial institutions were permitted to share nonpublic personal information, and has, in turn, highlighted the extent to which various entities buy, sell, and use nonpublic personal information; and
>
> WHEREAS, The Gramm-Leach-Bliley Act does not provide a comprehensive framework by which citizens may control access to their nonpublic personal information, but instead explicitly permits the states to enact laws that provide for greater protection of the privacy of nonpublic personal information; and
>
> WHEREAS, The citizens of California have indicated their great concern with this issue, and have made clear their overwhelming desire to have control over the disclosure of their nonpublic personal information; now, therefore, be it
>
> *Resolved by the Assembly of the State of California, the Senate thereof concurring,* That the Legislature authorizes and requests that the California Law Revision Commission study, report on, and prepare recommended legislation by January 1, 2005, if funding is provided in the 2002-03 Budget Act specifically for this purpose, concerning the protection of personal information relating to, or arising out of, financial transactions.

2002 Cal. Stat. res. ch. 167.

Current Legislative Activities Affecting GLB

California Legislature

The California Legislature has been a key forum in the debate between financial institutions and consumer interests over GLB's invitation to the states to

enact greater consumer protection. It is safe to say that this has been a major, if not the major, focus of lobbying activities for both groups during the past three years.

Legislation has been proposed that would prohibit a financial institution from sharing a customer's personal information with third parties unless agreed to by the customer ("opt in"), as opposed to the rule of GLB which would allow sharing unless prohibited by the customer ("opt out"). While legislation of this type has come very close to enactment, so far nothing has made it all the way through to become law.

A major effort will be made again in 2003. The focus is likely to be on SB 1 (Speier). The Commission's staff will follow the progress of this bill (and any others that may be introduced), and will report back to the Commission during the course of this study.

Local Public Entities

During fall of 2002, a number of local public entities enacted their own privacy ordinances, purporting to regulate privacy practices of financial institutions doing business within their jurisdictions. These measures basically track the opt in approach of bills introduced in the Legislature for sharing information with affiliates. The following jurisdictions have acted so far:

- San Mateo County
- Daly City
- Contra Costa County
- Alameda County
- City and County of San Francisco

The San Mateo County ordinance apparently serves as a model for the ordinances of the other local entities. The ordinances are being challenged in federal district court. See *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); *Bank of America, Wells Fargo, et al. v. Contra Costa*, No. 02-4943 (N.D. Cal.). The financial institutions argue that the ordinances are preempted by GLB, FCRA, and the National Bank Act, and are unconstitutional because they would have the effect of attempting to regulate transactions that occur outside their jurisdiction.

The staff will collect further information about these developments during the course of this study.

Ballot Initiative

There have been news reports that a ballot initiative campaign by consumer interests is likely if the Legislature is unable to enact satisfactory legislation during 2003. A successful initiative campaign requires a substantial investment of resources. However, the staff believes there is sufficient public interest and motivation concerning this matter that an initiative measure is a realistic possibility. We understand that one business executive has pledged $1 million to qualify a measure for the March 2004 ballot if the Legislature fails to act during 2003.

In North Dakota, a referendum to overturn a statute that had eroded North Dakota's strict financial privacy law obtained the support of 72% of the voters. It is reported that financial interests outspent consumer interests by five to one fighting the measure.

Perhaps the threat of a ballot initiative in California will be a catalyst to help precipitate an acceptable resolution in the Legislature in 2003.

Law Revision Commission Study

How does all this other activity impact the Commission's simultaneous study of the matter?

It is certainly not new for the Commission to study a topic while other legislative activities on that topic are progressing. The Commission has always taken the position that the fact of a Commission study should not in any way affect legislative activity to address the same matter. If legislation is enacted during the course of the Commission's study, the Commission's report will include an analysis of that legislation. If the Commission's study concludes that the legislation adequately addresses the issues, the Commission's report to the Governor and Legislature will so state. If the Commission's study concludes that not all issues are adequately addressed, or that improvements in the legislation can be made, the Commission's report will so state.

In the case of this particular project, the authorizing resolution addresses the matter directly:

> *Resolved*, That it is not the intent of the Legislature that enactment of this measure restrict the introduction, passage, or

operation of legislation relating to the financial service industry or related privacy issues.

2002 Cal. Stat. res. ch. 167.

It is clear that the Legislature contemplated the likelihood of simultaneous legislation, but nonetheless wants a careful and thorough report on the matter, of a type the Commission can provide.

GENERAL POLICY CONSIDERATIONS

Before we get into the specific policy issues and legal issues that will need to be resolved, it may be helpful to review some of the general policy arguments that may be involved in this study. How these will play out in the context of a particular financial privacy issue remains to be seen.

Some Policies That Support Restricted Use of Personal Financial Information

The California Constitution protects the right of privacy. Article I, Section 1 states that all people have inalienable rights, including the right to pursue and obtain privacy. In a sense, a person may be said to "own" the person's own personal information, or at least have a right to control use and dissemination of that information.

Much of the personal information we are concerned about is provided by the consumer to the financial institution. Other information is collected by a financial institution about a customer — account balances, spending habits, etc. However, a consumer enters into a financial transaction, and provides personal information for that transaction, with an expectation of confidentiality.

While it may reasonable to assume that a financial institution will use personal information to execute the financial transaction for which the information was provided, it may not be reasonable for that financial institution to in effect "convert" that information and use it for its own profit-making purposes. The consumer's consent to use of the information to facilitate a financial transaction cannot be construed as consent to "secondary use" of that information by the financial institution. Rather than appropriating personal information for commercial purposes, a financial institution should perhaps instead seek competitive market advantage by promising improved protection of customers' personal information.

While it may make sense to allow a consumer to waive privacy rights and agree to sharing of the consumer's personal information with third parties, that

should only be done with the informed consent of the consumer. Methods currently being used to inform the consumer and presume the consumer's consent, may be inadequate. Greater protection of privacy rights appears warranted.

Some Policies That Support More Liberal Use of Personal Financial Information

From the perspective of a financial institution, there is no need for additional state protections. Under federal law, the consumer can control dissemination of personal financial information by simply informing the financial institution with which the consumer does business.

The beneficial uses of personal information by financial institutions and the importance of information sharing — rapid and reliable availability of accurate and complete personal information — are essential to virtually all financial services. The benefits of information sharing, *when used responsibly*, include:

- Improving the speed, availability, and affordability of credit and other financial services.
- Providing efficient, reliable service.
- Identifying and meeting customer needs.
- Informing consumers of new opportunities.
- Preventing and detecting fraud.
- Ensuring solvency and facilitating safety.
- Improving efficiency and lowering costs.
- Serving the underserved.
- Promoting competition and helping small companies.
- Facilitating e-commerce and innovation.

Because of natural inertia, few consumers will exercise their rights, whether on an opt in or opt out basis. Thus an opt in system would do substantial damage because "it is impractical and prohibitively expensive to build and operate the systems that compare data in literally millions of accounts on an ad hoc basis. Virtually all of these information uses depend upon the routine availability of standardized, reliable, complete data. Moreover, the sheer cost of seeking consent would act as a dramatic disincentive to investing in innovation." Cate, *Personal Information in Financial Services: The Value of a Balanced Flow* (Financial Services Coordinating Council, March 2000).

Financial institutions have also made the argument that they have a constitutional right to share information — this is speech protected by the First Amendment to the United States Constitution. The courts that have considered this argument to date have not agreed. This sort of information is commercial speech and therefore entails reduced constitutional protection. Moreover, the governmental interest in protecting the privacy of consumer credit information is substantial and the governmental restrictions warranted. See, e.g., *Trans Union LLC v. Federal Trade Commission*, 295 F. 3d 42 (2002).

Fair Information Practice Principles

It is also worth reviewing "Fair Information Practice Principles" that are the basis for a number of privacy laws in various parts of the world. These principles were formulated by the United States Department of Health, Education and Welfare in 1973. They are reproduced here from the Organization for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*:

> **Openness.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> **Collection Limitation.** There should be limits to the collection of personal data and any such data should be obtain by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> **Purpose Specification.** The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> **Use Limitation.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified as described above, except with the consent of the data subject or by the authority of law.
>
> **Data Quality.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, relevant and kept up-to-date.
>
> **Individual Participation.** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to the

> individual; (b) to have communicated to the individual, data relating to the individual within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to the individual; (c) to be given reasons if a request is denied and to be able to challenge such denial; and (d) to challenge data relating to the individual and, if the challenge is successful, to have the data erased, rectified, completed or amended.
>
> **Security Safeguards.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> **Accountability.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

These principles have particular relevance in this study because part of the purpose of GLB is to promote the international competitiveness of United States financial institutions. See further discussion of "International Competition" below. However, as with any general statement of principle, they may cut either way as applied to particular issues and particular fact situations.

Empirical Data

It would be helpful to us also to have some data on information sharing practices among financial institutions and their affiliates. In fact, GLB § 6808 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.

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

So far as we can tell, the study is still underway. If it is released during the course of our project, it will undoubtedly be of substantial assistance to the Commission in making policy determinations.

FEDERAL FINANCIAL PRIVACY STATUTES

At the federal level, the two key financial privacy statutes are the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. The legislative resolution directing the present study requires that the legislation recommended by the Commission be compatible with, and withstand any preemption by, these two statutes.

Gramm-Leach-Bliley Act

The official title of the Gramm-Leach-Bliley Act is the "Financial Services Modernization Act of 1999". It was enacted by Public Law 106-102 (November 12, 1999). Chapter V of GLB, relating to disclosure of personal information, is found at 15 U.S.C. § 6801 et seq. The implementing Federal Trade Commission regulations are found at 16 C.F.R. 313 (May 24, 2002). The Federal Trade Commission has promulgated a useful summary of the provisions of GLB and implementing regulations, from which the following synopsis is drawn. A copy of the FTC Summary is attached at Exhibit p. 22.

Financial Institution

GLB governs the activities of "financial institutions". Under the statute and regulations, this includes any business institution that is significantly engaged in "financial activities" as described in the Bank Holding Company Act. The application of this standard is quite broad and would include, for example:

- 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

Even attorneys for whom tax advice or estate planning is a significant portion of their practice would be considered financial institutions under GLB. (More about this later.)

Consumer and Customer

A person dealing with a financial institution may have different privacy rights under GLB depending on whether the person is a consumer or a customer. A "consumer" is an individual who engages in a financial transaction such as applying for a loan, obtaining cash from an ATM, cashing a check, or arranging for a wire transfer. A "customer" is a consumer who is in a continuing relationship with a financial institution, such as opening a credit card account, entering into an automobile lease, obtaining a mortgage loan, or obtaining tax preparation or credit counseling services.

A consumer is entitled to notice that a copy of the financial institution's privacy policy is available, and a reasonable opportunity to opt out before personal information is shared with nonaffiliated third parties. A customer is entitled to an annual privacy notice for the duration of the customer relationship, and a reasonable opportunity to opt out before personal information is shared with nonaffiliated third parties.

Nonpublic Personally Identifiable Information

GLB limits only the sharing of nonpublic personally identifiable information. Examples of personally identifiable information of a consumer or customer include:

- Fact that an individual is the customer of a particular financial institution.
- Individual's name, address, social security number, account number.
- Any information individual provides on an application.
- Information from a "cookie" obtained in using a website.
- Information on a consumer report obtained by a financial institution. (Note: Such information may also be covered by the Fair Credit Reporting Act.)

However, there are no restrictions on sharing of personally identifiable information that is "public" such as:

- Fact that an individual is a mortgage customer of a particular financial institution where that fact is recorded in public real estate records.
- Telephone number listed in the phone book.
- Information lawfully available to the general public on a website (including a website that requires a password or fee for access).

Notice

Notices under GLB, whether to consumers or customers, and whether concerning privacy policies or an opportunity to opt out of sharing, must be clear and conspicuous, reasonably understandable, and designed to call attention to their content. These concepts are elaborated by regulation. The required content of the notices also is elaborated in some detail.

An opt out notice to a consumer or customer must contain the following information:

- Fact that the financial institution discloses (or reserves the right to disclose) nonpublic personal information about the individual to nonaffiliated third parties.
- The individual's right to opt out of those disclosures.
- A description of a "reasonable means" by which the individual can opt out, for example:

  Toll-free telephone number.

Detachable form with mailing information.

If the individual has agreed to receive notices electronically, an electronic means such as a form that can be sent via e-mail or through the financial institution's website.

Note: It is not a reasonable means to require an individual to write the individual's own letter as the only option.

(A financial institution must allow a "reasonable opportunity" for the individual to opt out before sharing information.)

Exceptions

There are major exceptions to the notice and opt out provisions of GLB that appear to swallow much of the rule.

A financial institution may share nonpublic personal information freely with its "affiliates", without notice or an opportunity to opt out. (More about affiliates later.)

A financial institution may also disclose nonpublic personal information to nonaffiliated third parties in a number of circumstances where a consumer or customer does not have the right to opt out of the sharing and, in some cases, will get no notice of the disclosure.

- Financial institution must provide notice but not the right to opt out when it provides nonpublic personal information to:

  Third party service provider that provides services for the financial institution; or

  Other financial institution(s) with whom the financial institution has entered into a joint marketing agreement.

  (Joint marketing agreement with other financial institution(s) means a written contract pursuant to which those institutions jointly offer, endorse, or sponsor a financial product or service.)

- Financial institution need not provide notice or obtain opt out when it discloses nonpublic personal information in the following circumstances:

  Disclosures necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes; or

  Disclosures made in connection with:

  Servicing or processing a financial product or service that a consumer requests or authorizes.

  Maintaining or servicing a consumer's account.

> A proposed or actual securitization, secondary market sale (including the sale of servicing rights) or similar transactions,

There are quite a few other exceptions whereby personally identifiable information may be disclosed by a financial institution that are tangential to the present study. For example, to resolve a consumer dispute, to persons acting in a fiduciary capacity on behalf of the consumer, to law enforcement (to the extent authorized by law), to comply with subpoena or other judicial process, etc.

However, a financial institution may not disclose, directly or through an affiliate, an account number of a consumer's credit card account, bank account, or transaction account to a nonaffiliated third party for use in marketing. A transaction account is an account to which a third party can initiate charges. (This rule applies even if the consumer gives express written consent to it. FTC, *Interp. Letter 910* (May 25, 2001).)

Reuse and Redisclosure

GLB also regulates reuse and redisclosure of nonpublic personal information by a third party that receives that information from a financial institution. Information received by a third party service provider or under a joint marketing agreement can only be used for the purpose for which it was disclosed. Redisclosure of information received for transactional purposes is similarly limited.

Otherwise, where a third party receives nonpublic personal information from a financial institution, after the institution has provided notice and an opt out opportunity but the consumer has not opted out, the third party may:

- Disclose the information to the affiliates of the financial institution from whom it received the information; or
- Disclose the information to its own affiliates, who are limited in their use of information in the same manner as the third party; or
- Disclose the information to any other entity consistent with the privacy policy of the financial institution from which it received the information.

Fair Credit Reporting Act

The Fair Credit Reporting Act ("FCRA") was enacted in 1970 as PL 91-508 (October 26, 1970), and is found at 15 U.S.C. § 1681. Its purpose 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.

To the extent FCRA authorizes financial institutions and credit bureaus to disclose personal financial information to each other, their affiliates, and third parties, it cuts across provisions of GLB. With respect to any conflict between the two laws, GLB expressly defers to FCRA. "[N]othing in this chapter shall be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act." 15 U.S.C. § 6806.

FCRA is extraordinarily complex, and it is beyond the scope of our present inquiry to summarize its full extent. Suffice it to say that, in general terms, the act regulates communication of information that bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. A credit bureau may provide information about a consumer to a person with a need recognized by the act — usually to consider an application with a creditor, insurer, employer, landlord, or other business. The consumer's consent is required before a credit bureau may provide information to an employer, or may make a report that includes medical information to a creditor, insurer, or employer.

A creditor or insurer may use file information as the basis for sending an unsolicited offer of credit or insurance. That type of offer must include a toll-free number by which the consumer may be taken off the solicitation list for two years. A consumer may also send a credit bureau a form requiring permanent removal from solicitation lists.

It is important to note for our purposes that FCRA regulates "consumer reports" — the communication of credit information about a consumer. The statute excludes from the definition of a consumer report the following types of communications:

- Any report containing information solely as to transactions or experiences between the consumer and the person making the report;
- Any communication of that information among persons related by common ownership or affiliated by corporate control; or
- Any 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 U.S.C. § 1681a(d)(2)(A).

Thus the limitations of FCRA do not apply to those types of communications. To the extent GLB regulates those types of communications, there would be no conflict between the two laws, and GLB would control. See, e.g., *Individual Reference Services Group, Inc. v. FTC*, 145 F. Supp. 2d 6 (2001), aff'd *Trans Union LLC v. FTC*, 295 F.3d 42 (2002).

An added complexity here is that GLB circles back and requires a financial institution's privacy notice to its customers to include "the disclosures required, if any" under the FCRA provision set out above. That certainly would require a financial institution to clearly and conspicuously disclose its policy on sharing information among its affiliates. Whether that would also require the financial institution to offer a consumer the opportunity to opt out of affiliate sharing — contrary to other provisions of GLB — is uncertain. The FTC regulations interpret this clause as merely a duplication of the FCRA notice, for informational purposes. To our knowledge, the issue has not yet been litigated.

USA Patriot Act

It is also worth noting the USA Patriot Act, enacted in the wake of the September 11, 2001, attacks. PL 107-56, 115 Stat. 272. The act exempts banks from privacy laws in order to share information concerning terrorism and money laundering. See, e.g., § 314(b):

> COOPERATION AMONG FINANCIAL INSTITUTIONS. — Upon notice provided to the Secretary, 2 or more financial institutions and any association of financial institutions may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the

> disclosure, except where such transmission, receipt, or sharing violates this section or regulations promulgated pursuant to this section.

This is one of many laws that override privacy statutes for law enforcement and related purposes. We do not plan to spend much time on statutes of this nature, other than to note their existence. It may be appropriate for proposed legislation to make clear that it is not intended to supersede statutory provisions of this type. See, e.g., SB 1 (Speier) (proposed Fin. Code § 4056(b)(12), making clear that release of nonpublic personal information is not prohibited if made pursuant to USA Patriot Act).

STATE FINANCIAL PRIVACY STATUTES

Other States

There has been recent activity in a number of states to enact legislation that protects consumer financial privacy. Attached at Exhibit p. 36 is a note from Elizabeth Huber, Chair of the Consumer Financial Services Committee of the State Bar Business Law Section, that provides us a synopsis of the activity in other states. (Ms. Huber's letter also includes a brief summary of the relevant federal law, and references to the California local ordinances.) The various state statutes may offer us a useful reference point on some of the issues that will come before us during this study.

Most of the state statutes are limited in scope. Comprehensive privacy bills that have been introduced in the past, but that have failed enactment, embrace common themes:

(1) They would prohibit a financial institution from sharing information with an affiliated entity, including an affiliate providing services on behalf of the financial institution.

(2) They would prohibit a financial institution from sharing information with a nonaffiliated entity, even though the two are operating under a joint marketing agreement.

(3) They would require a financial institution to obtain the consent ("opt in") of a customer before it may exchange information concerning the customer with an affiliated or nonaffiliated entity.

(4) They would require additional disclosure in a privacy notice provided to a customer or a consumer.

(5) They would prescribe monetary penalties for violation of the privacy protections.

(6) They would provide protection to a victim of identity theft.

SB 1 (Speier)

While California has no comprehensive financial privacy legislation in place, it is worth reviewing the key features of SB 1 (Speier). This bill is likely to be a focus of legislative attention during the 2003 session.

The complete text of the bill as introduced is set out at Exhibit p. 42. Key features of the bill, are:

- It would enact the California Financial Information Privacy Act. The act would preclude a financial institution from sharing nonpublic personal information of a consumer with a third party affiliated with the financial institution if the consumer opts out, and from sharing that type of information with a party not affiliated with the financial institution unless the consumer opts in.
- A financial institution would be required to give a statutorily prescribed form to the consumer specifying opt in and opt out choices. A financial institution would not be required to give the form to a consumer if the financial institution does not disclose nonpublic personal information to third parties.
- A financial institution could not deny a consumer a financial product or service because the consumer has not consented to the financial institution sharing nonpublic personal information.
- A financial institution could disclose nonpublic personal information to an affiliate or a nonaffiliated third party in order for it to perform certain services on behalf of the financial institution.
- The bill also provides for release of nonpublic personal information for various purposes, including identification or location of a missing child, witness, criminal or fugitive, party to a lawsuit, or missing heir. It would not change existing law regarding access by a law enforcement agency to information held by a financial institution.
- The bill would preempt local agency ordinances and regulations relating to the subject.
- The bill would provide civil penalties for negligent, or knowing and willful, violation of its provisions.

A survey of the legal issues we will need to address in the course of this study is in order. This survey is based on an initial review by the Commission staff. Obviously the survey cannot be comprehensive at this point in the project, but it can provide a starting point for Commission resolution of issues.

Scope of Project

General

The resolution directing this study requires the Commission to study, report on, and prepare recommended legislation concerning the protection of personal information relating to, or arising out of, financial transactions. 2002 Cal. Stat. res. ch. 167. The resolution does not define "financial transaction"; therefore it will be necessary for the Commission to delimit the scope of this project. The kinds of transactions that might be considered "financial" are potentially unlimited.

Because one of the objectives of the recommended legislation is to be compatible with, and withstand any preemption by, the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, the staff suggests that as an initial matter we limit the scope of the project to transactions that would be subject to those statutes. That would enable us to take advantage of definitional work already done under them. We could expand or contract the coverage of the study as the need becomes apparent during the course of the study.

Thus, coverage of the study would include such varied activities as:

- Leasing real or personal property or advising in such leasing
- Debt collecting
- Financial advisory actives, including management consulting and counseling
- Tax planning, preparation and advising

Attorneys and Others in a Confidential Relationship

One hotly contested aspect of GLB is its application to attorneys. An attorney may be substantially engaged in a tax or estate planning practice. FTC has taken the position that such an attorney is a "financial institution" within the meaning of GLB and must therefore send clients the annual privacy notice stating the attorney's policy on disclosing client personal information to affiliates and unaffiliated third parties, and offering clients an opportunity to opt out.

Attorneys have pointed out to FTC that state laws require absolute confidentiality — far more substantial than any provision of GLB — and therefore attorneys should be exempted from GLB. FTC has declined to exempt attorneys from coverage of the act, and the American Bar Association has now filed a lawsuit to void the FTC regulation.

The staff believes it is indisputable that, at least under California law, an attorney is required to protect personal financial information of a client to a far greater extent than would be required under federal law. See, e.g., Bus. & Prof. Code § 6068(e) (duty of attorney to "maintain inviolate the confidence, and a every peril to himself or herself to preserve the secrets" of a client).

It would make sense to exempt attorneys (and other professionals who are required by law to maintain client confidentiality) from the general statutes relating to financial privacy. In fact, SB 1 (Speier) would do just that:

> 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).

Why doesn't FTC directly exempt attorneys from application of GLB? FTC recognizes the argument, but doesn't believe the agency has authority to create such an exemption under the terms of GLB.

While the FTC may not be able to "exempt" attorneys from GLB, it may be able to determine that state law affords a person greater protection than GLB and therefore is not preempted by GLB. Whether such an FTC determination would excuse an attorney from compliance with the privacy notification requirements of GLB, absent state legislation to that effect, is unclear. For further discussion of preemption issues, see "Preemption" immediately below.

Preemption

The resolution directing this study requires that the recommendations of the Commission be compatible with, and withstand any preemption by, the Gramm-Leach-Bliley Act and the federal Fair Credit Reporting Act. We will review the situation with respect to each of these statutes.

As a matter of general law, in determining whether federal preemption exists, the principal inquiry of a court is the intention of Congress. State law may be preempted if it would stand as an obstacle to the accomplishment and execution

of the purposes and objectives of Congress, or if it conflicts with federal law such that compliance with both state and federal law is impossible. See, e.g., *English v. General Elec. Co.*, 496 U.S. 72, 78-79 (1990).

Gramm-Leach-Bliley Act

GLB includes express provisions concerning preemption. GLB does not supersede state law except to the extent state law is "inconsistent" with its provisions. State law is not inconsistent if the protection afforded a person by state law is greater than the protection provided by GLB, as determined by FTC. 15 U.S.C. § 6807. FTC has construed this provision to mean that state law is not inconsistent if the protection afforded a "consumer" is greater than the protection provided pursuant to GLB, as determined by FTC "on its own motion or upon the petition of any interested party." 16 C.F.R. § 313.17(b).

The policy expressed in GLB is 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 U.S.C. § 6801(a). Therefore, state law that provides greater privacy protection to consumers should generally be construed as "consistent" with GLB, and state law that seeks to cut back on privacy protection to consumers should generally be construed as "inconsistent" and preempted by GLB.

In fact FTC determinations pursuant to GLB have followed this line of reasoning. To date, FTC has ruled on preemption determination petitions concerning financial privacy laws of North Dakota and Connecticut. Petitions concerning Illinois and Vermont law are pending before FTC.

North Dakota. The North Dakota Disclosure of Customer Information law prohibits state-chartered financial institutions from disclosing customer information to any person, unless the customer has expressly consented to disclosure (opt in). State law does not prescribe the form or contents of written consent, but a customer may specify the time during which consent will be effective, the information to be disclosed, and the persons to whom information may be disclosed.

North Dakota added an exception to the statutory opt in requirement effective July 1, 2001. The new provision exempted from the requirements of the North Dakota statute "[a] disclosure of customer information by a financial institution to a nonaffiliated third party, if the disclosure is subject to federal law

on the date of the disclosure and the financial institution complies with applicable federal law in making the disclosure."

The FTC determination, issued June 28, 2001, is that the North Dakota statute as amended is not inconsistent with GLB. The preemption analysis focused on whether state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress" and whether it is possible for a private party to comply with both state and federal requirements. FTC noted that under the North Dakota statute, as amended, a state-chartered financial institution would not be required to comply with the opt in requirements under state law if the institution complies with the GLB Act. As a result, North Dakota law is not inconsistent with the opt out requirements under federal law.

North Dakota, by in effect gutting its opt in statute, did not provide a real test of state opt in legislation. Since that time, North Dakota voters, by referendum, have repealed the GLB compliance provision.

Connecticut. The Connecticut petition provided a better test before FTC. The privacy provisions under the Banking Law of Connecticut generally prohibit a financial institution from disclosing the financial records of a customer to any person unless the customer has authorized the disclosure (opt in). The Connecticut privacy provisions are narrower in scope than the privacy provisions under GLB, both as to the financial institutions covered under the state law and the information protected from disclosure.

The Connecticut law, as amended effective July 1, 2001, also requires a "financial institution" (as that term is defined under GLB) to comply with the privacy provisions of the GLB Act and the applicable implementing regulations, except to the extent that the federal law is inconsistent with the privacy provisions of state law. In the event of an inconsistency, the provisions affording greater protections to customers will be applicable.

The FTC determination, issued June 7, 2002, is that Connecticut law is not inconsistent with GLB and therefore is not preempted. The greater consumer protections provided by Connecticut law are consistent with the purpose of GLB to protect privacy of consumers, and it is physically possible for a financial institution to comply with both the federal and state requirements, by offering its customers an opt in choice.

Fair Credit Reporting Act

The Fair Credit Reporting Act regulates "consumer reports". A consumer report does not include any of the following:

- Any report containing information solely as to transactions or experiences between the consumer and the person making the report;
- Any communication of that information among persons related by common ownership or affiliated by corporate control; or
- Any 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.

See 15 U.S.C. § 1681a(d)(2)(A), discussed above under "Fair Credit Reporting Act".

Because these types of communications are not covered by FCRA, they are impliedly authorized by federal law. But would that fact preclude a state from stepping in and regulating those types of communications.

The staff believes it would be a stretch to extend federal preemption by FCRA to state regulation of those types of communications. The staff has not had the opportunity to fully research the issue. But the fact that a similar argument was rejected by a federal district court with respect to GLB regulation of "credit header" information that would otherwise be unregulated by FCRA is instructive. Credit bureaus had argued that because FCRA does not restrict dissemination of credit header information, the sale of that information is encompassed within the operation of FCRA and GLB cannot be construed to forbid what is permitted under FCRA. The federal court disagreed:

> Plaintiffs' argument is unpersuasive. Even assuming that 506(c) of the GLB Act is meant to preserve the effects of the FCRA, these effects are limited to the statutory and regulatory effects of the previous act and not the effects on private entities whose businesses are not addressed by the FCRA. In other words, Congress' decision not to regulate the disclosure of credit header information in the FCRA — or in any other statute prior to the enactment of the GLB Act — does not bestow upon plaintiffs the right to disclose that information in perpetuity free of governmental interference. While Congress may have been silent

> on an issue in the past, this does not amount to a waiver of its right to legislate on that subject in the future.

Individual Reference Services Group, Inc. v. FTC, 145 F. Supp. 2d 6 (2001), aff'd *Trans Union LLC v. FTC*, 295 F.3d 42 (2002) (savings clause does not prevent FTC from restricting credit bureau's disclosure either of types of information or under circumstances not enumerated in FCRA).

In any event, FCRA does not generally preempt a state statute governing collection, distribution, or use of information on consumers, except to the extent the statute is "inconsistent" with the act. 15 U.S.C. § 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 U.S.C. § 1681t(d). How the January 1, 2004, clause and the inconsistency clause interact with each other is not clear and may not become clear until tested after January 1, 2004.

It is worth noting, in this connection, that SJR 4 (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.

National Bank Act and Other Regulatory Regimes

Although the resolution directing this study does not refer to the National Bank Act or other federal regulatory regimes affecting financial institutions, an issue we must deal with in constructing sound state legislation is whether the National Bank Act and other federal statues may have a preemptive effect with respect to information sharing practices of financial institutions. Banks argue, for

example, that the National Bank Act is expansive in its grant of "incidental powers" (12 U.S.C. § 24(seventh)) that allow banks to market their services and to provide their subsidiaries the information necessary to operate competitively.

The Office of the Comptroller of the Currency ("OCC") has recently emphasized its "exclusive visitorial powers" over national banks and has alerted national banks to consult with OCC if state authorities seek to exercise enforcement powers over them. See *OCC Advisory Letter 2002-9* (11/25/02). OCC does not, in its advisory letter, expressly claim that state privacy laws are superseded by federal national banking laws, but the issue is there.

We are not in a position at this point to analyze these issues, but we will do so during the course of the study.

Local Ordinances

Do the same principles that apply to federal preemption of state law also apply to preemption of local ordinances? To the extent GLB specifically permits greater privacy protection by "a State statute, regulation, order, or interpretation", can this be construed to validate a local ordinance purporting to govern the matter? Apart from that, is it within the authority of a local entity to regulate privacy practices of a financial institution doing business within its jurisdiction?

The staff has not yet had the opportunity to research these issues. The staff believes, though, that it would not be in the interest of state commerce to have a hodge podge of inconsistent regulations bedeviling financial entities attempting to conduct business in the state. The staff suggests, as a feature of any recommended state legislation, that local regulations on the matter be preempted.

We note that SB 1 (Speier) includes a provision addressed to this point:

> 4058.5. This division shall preempt and be exclusive of all local agency ordinances and regulations relating to the use and sharing of nonpublic personal information by financial institutions. This section shall apply both prospectively and retroactively.

We assume that this sort of state preemption is permissible (despite city and county charter rights), but will research the matter further before this study is complete.

Interstate Commerce

Just as the staff thinks there is a concern with local entity regulation of financial privacy, we also think there may be a problem with inconsistent state regulation in the area. We can visualize a crazy-quilt of privacy regulation among the states that would make it a compliance nightmare for an entity seeking to engage in commerce on a national level. Of course, Congress had the opportunity to impose a single privacy regimen in GLB but elected not to do so. We have heard rumors that an effort may be made in Congress to forge a compromise that would amend GLB to provide greater privacy protection, in exchange for state preemption.

Meanwhile, this would seem to be an area where uniformity among the states would be beneficial. Perhaps a privacy article in the Uniform Commercial Code? This would be a worthwhile project for the National Conference of Commissioners on Uniform State Laws. Such a project would take some time, however.

SB 1 (Speier) offers a way to achieve some sort of consistency in the law, at least as between state and federal law. One of the purposes of that bill is to "adopt to the maximum extent feasible, definitions consistent with federal law, so that in particular there is no change in the ability of businesses to carry out normal processes of commerce for transactions voluntarily entered into by consumers." Proposed Fin. Code § 4051(b)(5).

The staff agrees with that approach, not only because it will facilitate compliance by business with the law, but also because it will help minimize complexity of the law in an area that is already extraordinarily complicated. The staff suggests that as a general principal, the Commission should adhere to existing federal categories and not create new ones unique to California. Unless, of course, there is a strong argument to depart from the federal scheme. See, e.g., discussion of "Affiliates" below.

Types of Information Controlled

If we adhere to the concept advocated above that we parallel federal categories, then the type of personal information controlled by state law would be "personally identifiable financial information" that is "nonpublic" in character. These concepts are elaborated in GLB and the implementing regulations, and would include such information as name, address, social

security number, assets, income, debt level, mortgage payments, income from child support payments, etc.

At least initially, that appears appropriate to the staff. The federal definitions make sense, and we have not seen any criticism of their coverage.

One question, though, is whether the general financial privacy provisions should supersede special statutes governing particular types of personal information. The special statutes might provide a different level of privacy protection — either stronger or weaker — than the general financial privacy statute.

For example, the Confidentiality of Medical Information Act (Civil Code Section 56 et seq.) governs privacy of medical information, which includes individually identifiable information, such as the patient's name, address, email address, telephone number, or social security number. Civ. Code § 56.05(f). Restrictions on disclosure of medical information may be stricter than restrictions on disclosure of financial information. See, e.g., Civ. Code § 56.26 (use and disclosure of medical and other information by third party administrators and others).

Probably we don't want the financial privacy statute to override provisions of this type, in the event a "financial institution" such as an insurer or a hospital credit department is involved. However, there are many statutes like this that will cut across the financial privacy statute, and listing each of them will be problematic. The staff suggests that we start with a presumptive rule that the general financial privacy statute not supersede any other conflicting state law. Before concluding our work, we should plan to examine every conflicting statute we can identify and confirm that policy is sound with respect to that statute.

Opt In v. Opt Out

The main debate over state regulation pursuant to GLB is whether to go beyond federal law in the extent to which consumer consent is required before a financial institution may share personal financial information with third parties. GLB allows a financial institution to share information with its affiliates, as well as with nonaffiliated third parties with which the financial institution has a joint marketing agreement, whether or not the consumer objects. GLB also allows a financial institution to share personal information with a nonaffiliated third party with which there is no joint marketing agreement, unless the consumer objects (opt out).

Affiliates

What is an "affiliate" of a financial institution? Recall that the main purpose of GLB was to break down the depression-era barriers between commercial banking, securities, and insurance industries. A financial institution may now merge with or acquire businesses in all of those fields. GLB defines an affiliate as a company that controls, is controlled by, or is under common control with, another company. The implementing regulations define "control" as 25% of the voting power, control of election of a majority of directors, or the power to exercise a controlling influence over company management or policies. 16 C.F.R. § 313.3(g) ("control" defined).

Why should it matter whether a financial institution discloses personal information to an affiliate or a nonaffiliate? On a theoretical level, it makes perfect sense for GLB to allow full disclosure among affiliates, since the purpose of GLB is to create financial supermarkets.

On a more practical level, should it make a difference how a corporation structures itself internally? Should it make a difference whether a corporation sets up internal divisions for handling customer services, as opposed to creating subsidiaries for the same purpose? Is there anything inherent in the corporate structure that would argue for limiting sharing of information within one type of corporate structure more than within another? In many cases, the particular corporate structure is determined by factors such as tax regulations or, in the case of operations in foreign countries, limitations on conduct of certain businesses by non-domestic firms.

While it may make sense to allow sharing of financial information among affiliates, this can be carried to an extreme. Citicorp, for example, has in excess of 1,900 affiliated companies. The Citicorp privacy notice refers to the "family of companies" to which it may disclose personal information, which encompasses companies engaged in "banking, credit cards, consumer finance, insurance, and securities" businesses.)

The authorizing resolution for this project directs the Commission to recommend legislation that will "provide consumers with notice and the opportunity to protect and control the dissemination of their personal information by, and between, companies and their affiliates and non-affiliated third parties." 2002 Cal. Stat. res. ch. 167. The staff takes this as a legislative policy decision that, unlike the rule under GLB, California consumers should have the opportunity to control affiliate sharing of their information.

A major decision for Commission resolution is whether sharing among affiliates should be precluded unless the consumer opts in, or should be allowed unless the consumer opts out. SB 1 (Speier) would take the opt out approach — its intent is to provide consumers with "the ability to prevent the sharing of financial information among affiliated companies through a simple opt out mechanism." Proposed Fin. Code § 5051.5(b)(3).

One issue the Commission may want to consider in this connection is whether the definition of "affiliate" under GLB regulations makes sense for information sharing purposes. If we assume the policy supporting more liberal information sharing among affiliates relates to internal communications within a single corporate structure, then an "affiliate" should really be a wholly-owned subsidiary of the financial institution. But under the GLB regulation, drawn from the Federal Reserve Act, a 25% ownership share of a company is sufficient to make the company an affiliate.

Thus an alternate approach for state law would be to tighten the definition of an affiliate, allow liberal information sharing within a true affiliate structure, and treat looser affiliations the same as nonaffiliated third parties for opt in or opt out purposes. Of course, this would violate the rule we have proposed above, of tracking federal definitions for logistical purposes.

Another way of looking at the issue, from a policy perspective, relates to the use to which the consumer information will be put. If the consumer provides information to a financial institution for the purpose of a particular transaction, shouldn't the financial institution be limited in its use of that information to that transaction. Why should a financial institution be authorized to use that information for secondary purposes — e.g., marketing other products to the consumer — without the consumer's consent, regardless of whether the financial institution is organized with or without internal divisions, and with or without affiliates?

The staff suggests that the Commission hold off on these issues for awhile. In particular, the approach taken may depend in part on the clarity required of the privacy notice and the ease with which opt in or opt out may be exercised.

Joint Marketing Agreements

Why would GLB, the avowed purpose of which is to protect the privacy of customer financial information, allow free sharing of that information among nonaffiliated companies, so long as they have a joint marketing agreement

between them? GLB provides that a financial institution may give nonpublic personal information to a nonaffiliated third party pursuant to a joint agreement between them under which they jointly offer, endorse, or sponsor a financial product or service. 15 U.S.C. §§ 6802(b)(2), 6809(10). In order to take advantage of this provision, the financial institution must disclose its practice in its privacy notice and the joint marketing agreement must restrict the nonaffiliated third party from further dissemination of the customer's information.

The apparent policy behind this provision is to level the playing field among large and small financial institutions. A larger financial institution may be able to expand its marketing reach by acquiring or merging with other entities, and using customer information internally. A smaller financial institution may not have the resources to do this, but may find it necessary to compete by entering into joint marketing agreements with other financial institutions.

It should be no surprise, then, that the joint marketing exemption was created at the request of small banks and credit unions. These small entities argued their need to do joint marketing to compete with large rivals that have broadened their product line by merging with insurers and security firms. For example, a smaller bank and another company could offer credit cards, or a credit card issuer might team up with an insurer to sell annuities or disability policies. The information sharing provision gives small banks the same ability to market products that a big bank has internally or through its affiliate structure.

This policy is specifically referred to in the resolution authorizing this study, which requires that among the objectives to be accomplished by the proposed legislation is:

> 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.

2002 Cal. Stat. res. ch. 167.

The policy is also recognized in SB 1 (Speier), which states that it is the intent of the Legislature:

> To provide a level playing field among types and sizes of businesses, including providing that those financial institutions with limited affiliate relationships may enter into agreements with other financial institutions on an "affiliate-equivalent" basis, as defined in statute, and providing that the different business models

> of differing financial institutions are treated in ways that provide consistent consumer control over information-sharing practices.

Proposed Fin. Code § 4051.5(b)(4). (Note that as introduced, the bill does not define "affiliate-equivalent".) The bill would allow sharing of personal information "for purposes of jointly offering a financial product or financial service pursuant to a written agreement" unless the consumer has opted out. Proposed Fin. Code § 4053(b)(2). In this connection, we understand that some banks currently allow customers to opt out of joint marketing agreements, even though not required by existing law.

If we assume that the concept is sound to treat joint marketing agreement information sharing as the equivalent of affiliate information sharing, then any tightening we might recommend for affiliate sharing should be accompanied by a corresponding tightening of joint marketing agreement sharing.

Unrelated Third Parties

The one aspect of information sharing that GLB does offer the consumer the ability to limit is sharing with nonaffiliated third parties. GLB requires that a consumer be notified of any such sharing that a financial institution proposes to engage in, and that the consumer be offered the opportunity to opt out of the sharing. 15 U.S.C. § 6802(b)(1). Recall that it was a scandal involving this type of information sharing that triggered inclusion of privacy protections at the time GLB was enacted. See discussion of "Growth of Privacy Concerns" above.

Financial institutions object to the privacy notification because it is wasteful. It is estimated that 25 billion privacy notices have been sent out so far; the average person will receive 18 privacy notices per year. In response to these notices, surveys suggest that approximately 40% of customers don't recall receiving the notice, 20% recall receiving the notice but didn't read it, and of the remainder who received and read the notice, only 2% have elected to opt out.

Consumer representative argue that the problem is not that people don't care, but that the privacy notices are too hard to understand — they are lengthy and characterized by fine print legalese. Opt out options are buried in the notices, which are designed to mislead and to discourage exercise of the opt out. The solution commonly advocated by consumer representatives is opt in — a financial institution may not share information with a nonaffiliated third party unless the consumer affirmatively agrees to it.

Financial institutions object that this is too draconian. The staff would like to see more convincing support for that position. Certainly, some states, as well as many foreign countries, have an opt in system without commerce coming to a standstill. Apart from reporting experience to a credit bureau for rating purposes (which is regulated by FCRA), what is the need of a financial institution to transfer personal information of its customers to an unrelated third party, other than simply to make money by providing the data? Granted, sale of customer data is a big business and an opt in requirement undoubtedly would destroy that business, but is that sufficient reason not to implement the public policy that favors protection of the confidentiality of consumer financial information? The arguments about the need to facilitate transactions do not apply where the transfer of information is to a nonaffiliated third party for purposes unrelated to the customer's relationship with the financial institution.

It may be that the argument here should boil down to the ease of election for the consumer. If the privacy notice makes it difficult for a consumer to make a choice, public policy would appear to favor opt in. If the privacy notice facilitates consumer choice, opt out would not appear to pose a serious problem.

Facilitate Transactions

The focus on sharing information among affiliated and nonaffiliated parties is perhaps a roundabout way of getting at a more fundamental consideration — what is the purpose for which a consumer has provided personal information to a financial institution, and should the financial institution be permitted to use that information for an unrelated or secondary purpose?

GLB recognizes this consideration, and does not provide for a consumer opt out of information sharing necessary to complete the transaction for which the information was provided, and for other purposes related to the transaction. This principle applies whether the sharing occurs with an affiliated or nonaffiliated party:

> 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)(1).

These categories appear to the staff to cut through affiliate/nonaffiliate considerations, and should be recognized by state law as permissible purposes for information sharing regardless of opt in or opt out considerations for other purposes. SB 1 (Speier) would do this also. See proposed Fin. Code § 4056(b).

Privacy Notices

Much of the opt in/opt out debate hinges on the adequacy of the privacy notice and the ease with which a consumer may make an informed choice. Although privacy notices have been criticized for their obfuscation, the staff has collected a few samples, most of which do not appear to be too bad. Of course what appears to a lawyer as "not so bad" may be total gibberish to a nonlawyer.

Nonetheless, the notices we have seen generally are written in plain English. While some are in small print, many are quite large and legible. Some include a form the consumer may use to opt out, others prominently feature a toll-free number. At least one notice contains both English and Spanish language versions, and provides a postage paid reply form for use in opting out.

Some companies take the opportunity in the notice to provide other privacy information, such as what to do in case of identity theft. A number of the notices indicate that customer privacy is a priority for the company, and that the company not share personal information with third parties at all.

Part of the concern with privacy notices relates to the fact that the consumer may not appreciate the practical consequences of the information being conveyed. If a notice states that a company will not share information except with affiliates, the consumer does not necessarily understand that this may include a very broad range of unrelated companies, for unrelated purposes.

One approach to the privacy notice issue would be for state law to prescribe requirements over and above federal minimums in order to facilitate the intended purpose of providing clear information and an informed choice for consumers. SB 1 (Speier), for example, would prescribe a statutory form that must be returned before a financial institution may share consumer information.

Another approach would be to forget about upgrading privacy notices and focus instead on "do not call" lists. That would attack the concern of many consumers — telemarketing — directly rather than indirectly. (Junk mail does not appear to be as significant an issue for many consumers.) Of course, that would not address the more generalized privacy and identify-theft concerns that consumers may have about vulnerability of their personal information.

International Competition

One of the purposes of GLB is to facilitate the ability of financial institutions to compete globally with foreign banking companies. By the same token, United States companies will need to comply with foreign privacy protection laws in order to do business abroad. Does this fact argue for drawing our laws in such a way as to facilitate compliance with international privacy standards?

A useful compendium of privacy principles applicable to European transactions may be found in the "EU Safe Harbor" developed by the U.S. Department of Commerce. Domestic companies that subscribe to the safe harbor principles may be assured of compliance with European directives. The safe harbor principles are:

> **Notice**: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can 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 for limiting its use and disclosure.
>
> **Choice**: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.
>
> **Onward Transfer (Transfers to Third Parties)**: To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.
>
> **Access**: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case

in question, or where the rights of persons other than the individual would be violated.

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

Perhaps the most interesting aspect of the safe harbor principles for our present purposes is the provision giving an individual the right to control information transfers to third parties. Opt in and opt out determinations are based not on the relationship between the transferor and transferee, but on the type of information transferred.

Under the principles, an individual must be given an opt out opportunity generally, but in any event "sensitive information" cannot be transferred unless the individual opts in. The full text of the sensitive information principle is set out below:

Safe Harbor Sensitive Information Principle: For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received

> from a third party where the third party treats and identifies it as sensitive.

Financial information would not be categorized as "sensitive" for opt in purposes. (Unless the consumer identifies the information as sensitive. But if the consumer goes to that trouble, why not just opt out to begin with and be done with it?)

State Regulators

Does it make sense to micromanage by statute issues such as the form and content of privacy notices, or the percentage ownership required in order to qualify as a controlled affiliate? In fact, under GLB, issues such as these are resolved by administrative regulation.

The resolution directing the present study contemplates a role for state regulators in this field. The proposed legislation should:

> 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.

2002 Cal. Stat. res. ch. 167. The concept here is that state law would prescribe the general policy framework, which would be fleshed out and implemented by regulation.

An added consideration relating to use of regulations, rather than detailed statutes, is that all aspects of the governing law in this field are tied to federal regulations. If the federal regulations change, that may necessitate a change in state law. A state regulatory regimen could be more responsive in this situation.

One concern we have heard expressed is that important public policies such as protection of personal information should not be left to regulators who may be political appointees or may be "captive" to the industry they purport to regulate. The staff has no sense of the extent to which this is a real problem in the area of financial regulation.

Obviously, the breadth of commerce that could be considered "financial" is such that any of a number of regulators might be considered appropriate. Just on the surface of banking, securities, and insurance industries, there are a number of state-level regulators that might logically be involved. Under GLB, for example,

regulatory and enforcement authority is delegated to seven different federal agencies, depending on the particular industry being regulated:

- Federal Trade Commission
- Office of the Comptroller of the Currency
- Board of Governors of the Federal Reserve System
- Board of Directors of the Federal Deposit Insurance Corporation
- Director of the Office of Thrift Supervision
- Board of the National Credit Union Administration
- Securities and Exchange Commission

Obviously, as politics change and political appointees change, an administrative agency my be more or less vigorous in its attitude toward regulation. But if the policy of the law is stated with sufficient specificity, there should be no concern about fleshing out the details through regulation.

The staff is not prepared at this point to suggest what issues should be left to regulatory authority, or which regulatory authority should be designated. However, the Commission should bear in mind as we work our way through the issues that we need not necessarily detail every aspect of the financial privacy law by statute, and that the Legislature has contemplated the possibility of delegating some matters to regulatory authority.

Remedies

The resolution authorizing this study requires that the proposed legislation:

> 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.

By comparison, GLB provides no private right of action for violation of its provisions, but administrative remedies only. 15 U.S.C. § 6805. Typical federal administrative enforcement remedies include injunctive relief and cease and desist powers.

In general, the staff would expect that a judicial proceeding for actual and compensatory damages is not an effectual enforcement mechanism in this area. Proof of damages could be problematic. Generally speaking, the cost of individual litigation to remedy a privacy violation would be prohibitive for the ordinary consumer. An award of attorney's fees would help in this respect, as would authorization of exemplary damages. The Commission will need to decide whether to propose a separate attorney's fee authorization, or to recommend treatment of this litigation within standard categories, such as the "private attorney general" statute. See Code Civ. Proc. § 1021.5.

Civil penalties contemplated by the legislative resolution would likewise assist individual enforcement of privacy rights. It is worth noting that SB 1 (Speier) would provide a civil penalty for a financial privacy violation of up to $2,500, with the amount doubled in case the violation results in identity theft. See proposed Fin. Code § 4057.

The Commission is quite familiar with the unfair competition law and its problems. See *Unfair Competition Litigation*, 26 Cal. L. Revision Comm'n Reports 191 (1996). An effort may be made during the 2003 legislative session to cure some of the current abuses occurring under the statute. See, e.g., AB 69 (Correa) (spot bill). The staff would be reluctant to foster use of the unfair competition statute to address financial privacy violations unless the problems with the statute are also addressed. The Commission's corrective recommendations for the unfair competition law are:

- A plaintiff seeking to represent the general public would have to be an adequate representative of the interest of the general public pled and meet basic conflict of interest standards.
- The plaintiff's attorney would have to be an adequate legal representative of the interests of the general public pled in the action.
- Notice of commencement of a private representative action, and notice of proposed terms of a judgment, would be given to the Attorney General and district attorney. Notice of the proposed terms of the judgment would also be given to parties in other similar cases against the defendant.
- A fairness hearing would be held to make sure that the judgment in a private representative action is "fair, reasonable, and adequate" to protect the interests of the general public. Interested persons would be permitted to appear and comment on the proposed terms.

- The determination of a private representative claim on behalf of the general public would bar any further private representative claims on that cause of action. Any right to sue for individual claims would not be affected by this rule.
- Prosecutors would be given a degree of procedural priority over private plaintiffs in representing the public. The right of the private plaintiff to attorney's fees is recognized in cases where a private plaintiff contributes to a prosecutor's action.

Administrative enforcement of privacy statutes could perhaps be more efficacious than private enforcement. Administrative penalties could be combined with other administrative enforcement mechanisms. These we would develop later, depending on the regulatory agency or agencies selected for enforcement of the state financial privacy law. One concern with administrative enforcement as an exclusive remedy is the current state budget shortfall and the likelihood that state regulatory agency operations will be severely curtailed.

Jurisdictional Issues

The staff has not seen any discussion of jurisdictional issues relating to state regulation of financial institutions doing business in the state. Presumably the concepts are so well settled by now that it is not a concern. But to the extent a financial transaction is conducted electronically, by an entity that may have no physical presence in the state, the staff wonders whether the law is sufficiently clear, particularly as it relates to long-arm jurisdiction for enforcement of rights in state courts.

Obviously, we will not resolve this developing area of law in the context of this particular study. Probably the best approach will be to provide general rules, and let the constitutional limits on jurisdiction work themselves out. But it is an issue we should be sensitive to as we proceed through this study. It may make some sense to require regulations to define the term "doing business in this state" or whatever the statutory phrase ultimately turns out to be.

Retroactivity

Any change in law must deal with the fact that much information has already changed hands, and continues to change hands under agreements entered into under old law. This poses both practical and legal concerns.

As a practical matter, much personal information is already out there. But this does not mean that it is pointless to provide a satisfactory means of enabling a consumer to limit future transfers of personal information. After all, new

accounts are opened all the time, and new transactions entered into. Just because old information may already be in the stream of commerce is no reason automatically to allow new information into the stream. To the extent new law may be more responsive to parties' interests, the staff believes there is plenty of value to be achieved.

Can new laws affect existing information sharing agreements involving financial institutions, or must they be prospective only in their operation? At least on the surface it appears there could be constitutional impairment of contractual obligation issues here. U.S. Const. Art. I, § 10(1). The staff will develop this matter later in the study, after the Commission's direction becomes clear.

CONCLUSION

There are common principles of fair information that appear to be generally accepted and used in many laws both in the United States and in other countries. They include disclosure, consent, access, security, collection limitation, accountability, and secondary use restrictions. These principles can be found, for example, in GLB, FCRA, and the EU Safe Harbor.

As always, the devil is in the details. What form, for example, should "consent" take — opt in or opt out — and for what type of information or transfer? The task that has been assigned the Law Revision Commission is to propose appropriate implementing legislation consistent with the general principles.

A substantial body of excellent work has already been done in this area. The staff thinks it is likely that comprehensive implementing legislation will be enacted in California during the course of this project — probably by the Legislature, but possibly by initiative measure. In that event, the Commission's final report to the Legislature should focus on what further improvements to the law, if any, should be made.

Respectfully submitted,

Nathaniel Sterling
Executive Secretary

Assembly Concurrent Resolution No. 125

RESOLUTION CHAPTER 167

Assembly Concurrent Resolution No. 125—Relative to the protection of personal information.

[Filed with Secretary of State September 16, 2002.]

LEGISLATIVE COUNSEL'S DIGEST

ACR 125, Papan. Relative to the protection of personal information.

This measure would request and authorize the California Law Revision Commission to study, report on, and prepare recommended legislation concerning the protection of personal information relating to or arising out of financial transactions if funding is provided in the 2002-03 Budget Act. The measure would direct that the recommended legislation address specified objectives.

WHEREAS, The Financial Services Modernization Act, commonly known as the Gramm-Leach-Bliley Act, became law in 1999, and reformed the laws that define and regulate the structure of the financial services industry; and

WHEREAS, The Gramm-Leach-Bliley Act greatly liberalized the ways that financial institutions were permitted to share nonpublic personal information, and has, in turn, highlighted the extent to which various entities buy, sell, and use nonpublic personal information; and

WHEREAS, The Gramm-Leach-Bliley Act does not provide a comprehensive framework by which citizens may control access to their nonpublic personal information, but instead explicitly permits the states to enact laws that provide for greater protection of the privacy of nonpublic personal information; and

WHEREAS, The citizens of California have indicated their great concern with this issue, and have made clear their overwhelming desire to have control over the disclosure of their nonpublic personal information; now, therefore, be it

Resolved by the Assembly of the State of California, the Senate thereof concurring, That the Legislature authorizes and requests that the California Law Revision Commission study, report on, and prepare recommended legislation by January 1, 2005, if funding is provided in the 2002–03 Budget Act specifically for this purpose, concerning the protection of personal information relating to, or arising out of, financial transactions, and that this legislation shall accomplish the following objectives:

(a) Provide consumers with notice and the opportunity to protect and control the dissemination of their personal information by, and between, companies and their affiliates and non-affiliated third parties;

(b) 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;

(c) 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;

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

(e) 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; and be it further

Resolved, That it is not the intent of the Legislature that enactment of this measure restrict the introduction, passage, or operation of legislation relating to the financial service industry or related privacy issues; and be it further

Resolved, That the Chief Clerk of the Assembly transmit copies of this resolution to the California Law Revision Commission and to the author for appropriate distribution.

O

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

OFFICE OF
Privacy Protection

Privacy Laws

This page contains links to some of the major privacy protection laws at the State and federal level. The site will be updated periodically to add other privacy-related laws and to reflect changes in the laws.

▶ Fair Information Practice Principles
These widely accepted Fair Information Practice Principles are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world.

▶"Safe Harbor" Privacy Framework
Unlike the U.S. approach to privacy protection, which relies on industry-specific legislation, regulation and self-regulation, the European Union relies on comprehensive privacy legislation. The European Directive on Data Protection that went into effect in October 1998, includes, for example, the requirement to create government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor - approved by the EU in July of 2000 - is a way for U.S. companies to comply with European privacy laws.

California Laws

▶ California Constitution, Article 1, Section 1 The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

▶ Credit Card Number Truncation - California Civil Code Section 1747.9 No more than the last five digits of a credit card number may be printed on electronic receipts. Effective 1/1/01 for machines put in use on or after that date. Effective 1/1/04 for all machines that electronically print credit card receipts.

▶ Confidentiality of Medical Information Act - California Civil Code Sections 56-56.37 This law puts limits on the disclosure of patients' medical information by medical providers and health plans.
www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20

▶ Confidentiality of Social Security Numbers - California Civil Code Section 1798.85 and 1786.6 This law restricts businesses from publicly posting or displaying Social Security numbers. The law takes effect gradually from 7/1/02 through 7/1/05.

▶ Consumer Credit Reporting Agencies Act Civil Code Section 1785.1-1785.35 - This law, the state counterpart of the Fair Credit Reporting Act, regulates consumer credit reporting agencies. It requires them, among other things, 1) to provide free copies of credit reports to consumers who have been denied credit or who are identity theft victims, 2) to block information that appears on a report as the result of identity theft, 3) to place security alerts (effective 7/1/02) or freezes (effective 1/1/03) on the files of consumers who request them, and 4) to provide, for a reasonable fee, credit score information to consumers who request it.

▶ Destruction of Customer Records - California Civil Code Sections 1798.80 - 1798.82 This requires businesses to shred, erase or otherwise modify the personal information in records under their control.

▶ Identity Theft: Access to Financial Records on Fraudulent Accounts - California Civil Code Section 1748.95, California Financial Code Sections 4002 and 22470. Similar to Penal Code section 530.8, these laws require certain types of financial institutions to release (to a victim with a police report or to the victim's law enforcement representative) information and evidence related to identity theft.

▶ Identity Theft - California Penal Code Sections 530.5-530.8
These code sections define the specific crime of identity theft, require the law enforcement agency in the victim's area to take a police report, allow a victim to get an expedited judicial ruling of factual innocence, require the Department of Justice to establish a database of identity theft victims accessible by law enforcement and victims, and require financial institutions to release information and evidence related to identity theft to a victim with a police report or to the victim's law enforcement representative.

▶ Identity Theft Victim's Rights Against Claimants - Civil Code Section 1798.92-1798.97 This law protects identity theft victims who are being pursued for collection of debts which have been created by identity thieves. The law gives identity theft victims the right to bring an action against a claimant who is seeking payment on a debt NOT owed by the identity theft victim. The identity theft victim may seek an injunction against the claimant, plus actual damages, costs, a civil penalty, and other relief.

▶Information Practices Act of 1977- California Civil Code Sections 1798 and following This law applies to state government. It expands upon the constitutional guarantee of privacy by providing limits on the collection, management and dissemination of personal information by state agencies.

▶ Investigative Consumer Reporting Agencies Act, California Civil Code Sections 1786-1786.60 This law regulates the activities of agencies that collect information on consumers for employers, insurance companies and landlords.

▶ Legal and Civil Rights of Persons Involuntarily Detained - Welfare & Institutions Code Section 5328 This law provides for the confidentiality of the records of people who are voluntarily or involuntarily detained for psychiatric evaluation or treatment.

▶ Mandated Blood Testing and Confidentiality to Protect Public Health - California Health & Safety Code Sections 120975-121020
This law protects the privacy of individuals who are the subject of blood testing for antibodies to the probable causative agent of acquired immune deficiency syndrome (AIDS).

▶ Office of Privacy Protection - California Business and Professions Code Section 350-352 A state law enacted in 2000 created the Office of Privacy Protection, with the mission of protecting and promoting the privacy rights of California consumers.
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=00001-01000&file=350-352

▶Patient Access to Medical Records - California Health & Safety Code Section 123110 et seq.
With minor limitations, this law gives patients the right to see and copy information maintained by health care providers relating to the patients' health conditions. The law also gives patients the right to submit amendments to their records, if the patients believe that the records are inaccurate or incomplete.>

▶ Personal Information Collected on Internet - California Government Code Section 11015.5 This law applies to state government agencies. When collecting personal information electronically, agencies must provide certain notices. Before sharing an individual's information with third parties, agencies must obtain the individual's written consent.

▶ Public Records Act - California Government Codes Sections 6250-6268 This law applies to state and local government. It gives members of the public a right to obtain certain described kinds of documents that are not protected from disclosure by the Constitution and other laws. It also requires that state and local agencies be "mindful" of the laws that confer privacy rights. This law also provides some specific privacy protections.

▶ Spam laws - California Business and Professions Code, Section 17538.4 and 17538.45 - Penal Code Section 502 These code section establish the guidelines relating to unsolicited e-mail and faxes.

Federal Laws

▶ Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code 6501 et seq. The Act's goal is to place parents in control over what information is collected from their children online. With limited exceptions, the related FTC Rule requires operators of commercial websites and online services to provide notice and get parent's consent before collecting personal information from children under 13.

▶ Driver's Privacy Protection Act of 1994 - 18 U.S. Code 2721 et seq. This law puts limits on disclosures of personal information in records maintained by departments of motor vehicles.

▶ Fair Credit Reporting Act (FCRA) - 15 USC 1681-1681u
This federal law is designed to promote accuracy, fairness, and privacy of information in the files of every "consumer reporting agency," the credit bureaus that gather and sell information about consumers to creditors, employers, landlords and other businesses.
www.ftc.gov/bcp/conline/edcams/fcra/index.html

▶ Family Educational Rights and Privacy Act of 1974 (FERPA) - 20 U.S. Code 1232g This law puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.

▶ Federal Identity Theft Assumption and Deterrence Act of 1998 - 18 USC 1028 The Act makes it a federal crime to use another's identity to commit an activity that violates Federal law or that is a felony under State or local law. Violations are investigated by federal agencies including the Secret Service, the FBI and the Postal Inspection Service and prosecuted by the U.S. Department of Justice. www4.law.cornell.edu/uscode/18/1028.html

▶ Federal Privacy Act of 1974 - 5 U.S. Code 552a This law applies to the records of federal government executive and regulatory agencies. It requires such agencies to apply basic fair information practices to records containing the personal information of most individuals.

▶ Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule - 15 USC 6801-6827 The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies.
www.ftc.gov/privacy/glbact/index.html

▶ Health Information Portability and Accountability Act of 1996 (HIPAA), Standards for Privacy of Individually Identifiable Health Information, Final Rule - 45 CFR Parts 160 and 164 HIPAA includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the security and confidentiality of patient information. The privacy rule took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply. http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy

▶ Telephone Consumer Protection Act (TCPA) - 47 U.S. Code 227 This law puts restrictions on telemarketing calls and on the use of autodialers, prerecorded messages, and fax machines to send unsolicited advertisements.

Updated December 12, 2002

Office of Privacy Protection
400 R Street, Suite 3000
Sacramento, CA 95814
Toll Free
(866) 785-9663
www.privacy.ca.gov
email:privacy@dca.ca.gov

EX 4

Gramm-Leach-Bliley Act
15 USC, Subchapter I, Sec. 6801-6810
Disclosure of Nonpublic Personal Information

Sec. 6801. Protection of nonpublic personal information

(a) Privacy obligation policy

It is the policy of the 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.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards -

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6803, 6805 of this title.

Sec. 6802. Obligations with respect to disclosures of personal information

(a) Notice requirements

Except as otherwise provided in this subchapter, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title.

(b) Opt out

(1) In general

A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless -

(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the

regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party;

(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and

(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.

(2) Exception

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.

(c) Limits on reuse of information

Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.

(d) Limitations on the sharing of account number information 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.

(e) General exceptions

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.

(Pub. L. 106-102, title V, Sec. 502, Nov. 12, 1999, 113 Stat. 1437.)

REFERENCES IN TEXT

This subchapter, referred to in subsecs. (a) and (c), was in the original "this subtitle", meaning subtitle A (Sec. 501 et seq.) of title V of Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1436, which enacted this subchapter and amended section 1681s of this title.

For complete classification of subtitle A to the Code, see Tables.

The Right to Financial Privacy Act of 1978, referred to in subsec. (e)(5), is title XI of Pub. L. 95-630, Nov. 10, 1978, 92 Stat. 3697, as amended, which is classified generally to chapter 35 (Sec. 3401 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 3401 of Title 12 and Tables.

Chapter 2 of title I of Public Law 91-508, referred to in subsec. (e)(5), is chapter 2 (Sec. 121-129) of title I of Pub. L. 91-508, Oct. 26, 1970, 84 Stat. 1116, which is classified generally to chapter 21 (Sec. 1951 et seq.) of Title 12, Banks and Banking. For complete classification of chapter 2 to the Code, see Tables.

The Fair Credit Reporting Act, referred to in subsec. (e)(6)(A), is title VI of Pub. L. 90-321, as added by Pub. L. 91-508, title VI, Sec. 601, Oct. 26, 1970, 84 Stat. 1127, as amended, which is classified generally to subchapter III (Sec. 1681 et seq.) of chapter 41 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6803, 6804, 6809 of this title.

Sec. 6803. 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.

(Pub. L. 106-102, title V, Sec. 503, Nov. 12, 1999, 113 Stat. 1439.)

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 6802 of this title.

Sec. 6804. Rulemaking

(a) Regulatory authority

(1) Rulemaking

The Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission shall each prescribe, after consultation as appropriate with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, such regulations as may be necessary to carry out the purposes of this subchapter with respect to the financial institutions subject to their jurisdiction under section 6805 of this title.

(2) Coordination, consistency, and comparability

Each of the agencies and authorities required under paragraph (1) to prescribe regulations shall consult and coordinate with the other such agencies and authorities 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.

(3) Procedures and deadline

Such regulations shall be prescribed in accordance with applicable requirements of title 5 and shall be issued in final form not later than 6 months after November 12, 1999.

(b) Authority to grant exceptions

The regulations prescribed under subsection (a) of this section may include such additional exceptions to subsections (a) through (d) of section 6802 of this title as are deemed consistent with the purposes of this subchapter.

(Pub. L. 106-102, title V, Sec. 504, Nov. 12, 1999, 113 Stat.1439.)

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6802, 6803, 6809 of this title.

Sec. 6805. Enforcement

(a) In general

This subchapter and the regulations prescribed thereunder shall be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction under applicable law, as follows:

(1) Under section 1818 of title 12, in the case of -

(A) national banks, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 et seq., 611 et seq.), and bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Governors of the Federal Reserve System;

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System), insured State branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Board of Directors of the Federal Deposit Insurance Corporation; and

(D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers), by the Director of the Office of Thrift Supervision.

(2) Under the Federal Credit Union Act (12 U.S.C. 1751 et seq.), by the Board of the National Credit Union Administration with respect to any federally insured credit union, and any subsidiaries of such an entity.

(3) Under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.), by the Securities and Exchange Commission with respect to any broker or dealer.

(4) Under the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.), by the Securities and Exchange Commission with respect to investment companies.

(5) Under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.), by the Securities and Exchange Commission with respect to investment advisers registered with the Commission under such Act.

(6) Under State insurance law, in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 6701 of this title.

(7) Under the Federal Trade Commission Act (15 U.S.C. 41 et seq.), by the Federal Trade Commission for any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under paragraphs (1) through (6) of this subsection.

(b) Enforcement of section 6801

(1) In general

Except as provided in paragraph (2), the agencies and authorities described in subsection (a) of this section shall implement the standards prescribed under section 6801(b) of this title in the same manner, to the extent practicable, as standards prescribed pursuant to section 1831p-1(a) of title 12 are implemented pursuant to such section.

(2) Exception

The agencies and authorities described in paragraphs (3), (4), (5), (6), and (7) of subsection (a) of this section shall implement the standards prescribed under section 6801(b) of this title by rule with respect to the financial institutions and other persons subject to their respective jurisdictions under subsection (a) of this section.

(c) Absence of State action

If a State insurance authority fails to adopt regulations to carry out this subchapter, such State shall not be eligible to override, pursuant to section 1831x(g)(2)(B)(iii) of title 12, the insurance customer protection regulations prescribed by a Federal banking agency under section 1831x(a) of title 12.

(d) Definitions

The terms used in subsection (a)(1) of this section that are not defined in this subchapter or otherwise defined in section 1813(s) of title 12 shall have the same meaning as given in section 3101 of title 12.

(Pub. L. 106-102, title V, Sec. 505, Nov. 12, 1999, 113 Stat. 1440.)

REFERENCES IN TEXT

Section 25 of the Federal Reserve Act, referred to in subsec. (a)(1)(B), is classified to subchapter I (Sec. 601 et seq.) of chapter 6 of Title 12, Banks and Banking. Section 25A of the Federal Reserve Act is classified to subchapter II (Sec. 611 et seq.) of chapter 6 of Title 12.

The Federal Credit Union Act, referred to in subsec. (a)(2), is act June 26, 1934, ch. 750, 48 Stat. 1216, as amended, which is classified generally to chapter 14 (Sec. 1751 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see section 1751 of Title 12 and Tables.

The Securities Exchange Act of 1934, referred to in subsec. (a)(3), is act June 6, 1934, ch. 404, 48 Stat. 881, as amended, which is classified principally to chapter 2B (Sec. 78a et seq.) of this title. For complete classification of this Act to the Code, see section 78a of this title and Tables.

The Investment Company Act of 1940, referred to in subsec. (a)(4), is title I of act Aug. 22, 1940, ch. 686, 54 Stat. 789, as amended, which is classified generally to subchapter I (Sec. 80a-1 et seq.) of chapter 2D of this title. For complete classification of this Act to the Code, see section 80a-51 of this title and Tables.

The Investment Advisers Act of 1940, referred to in subsec. (a)(5), is title II of act Aug. 22, 1940, ch. 686, 54 Stat. 847, as amended, which is classified generally to subchapter II (Sec. 80b-1 et seq.) of chapter 2D of this title. For complete classification of this Act to the Code, see section 80b-20 of this title and Tables.

The Federal Trade Commission Act, referred to in subsec. (a)(7), is act Sept. 26, 1914, ch. 311, 38 Stat. 717, as amended, which is classified generally to subchapter I (Sec. 41 et seq.) of chapter 2 of this title. For complete classification of this Act to the Code, see section 58 of this title and Tables.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 6801, 6804, 6807 of this title.

Sec. 6806. Relation to other provisions

Except for the amendments made by subsections (a) and (b), nothing in this chapter 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 chapter regarding whether information is transaction or experience information under section 603 of such Act (15 U.S.C. 1681a).

(Pub. L. 106-102, title V, Sec. 506(c), Nov. 12, 1999, 113 Stat. 1442.)

REFERENCES IN TEXT

Amendments made by subsections (a) and (b), referred to in text, means amendments made by section 506(a) and (b) of Pub. L. 106-102, which amended section 1681s of this title.

This chapter, referred to in text, was in the original "this title", meaning title V of Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1436, as amended, which enacted this chapter and amended section 1681s of this title. For complete classification of title V to the Code, see Tables.

The Fair Credit Reporting Act, referred to in text, is title VI of Pub. L. 90-321, as added by Pub. L. 91-508, title VI, Sec. 601, Oct. 26, 1970, 84 Stat. 1127, as amended, which is classified generally to subchapter III (Sec. 1681 et seq.) of chapter 41 of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of this title and Tables.

Sec. 6807. 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.

(Pub. L. 106-102, title V, Sec. 507, Nov. 12, 1999, 113 Stat. 1442.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle A (Sec. 501-510) of title V of Pub. L. 106-102, Nov. 12, 1999, 113 Stat. 1436, which enacted this subchapter and amended section 1681s of this title. For complete classification of subtitle A to the Code, see Tables.

Sec. 6808. Study of information sharing among financial affiliates

(a) In general

The Secretary of the Treasury, in conjunction with the Federal functional regulators and the Federal Trade Commission, shall conduct a study of information sharing practices among financial institutions and their affiliates. Such study shall include -

(1) the purposes for the sharing of confidential customer information with affiliates or with nonaffiliated third parties;

(2) the extent and adequacy of security protections for such information;

(3) the potential risks for customer privacy of such sharing of information;

(4) the potential benefits for financial institutions and affiliates of such sharing of information;

(5) the potential benefits for customers of such sharing of information;

(6) the adequacy of existing laws to protect customer privacy;

(7) the adequacy of financial institution privacy policy and privacy rights disclosure under existing law;

(8) 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; and

(9) the feasibility of restricting sharing of information for specific uses or of permitting customers to direct the uses for which information may be shared.

(b) Consultation

The Secretary shall consult with representatives of State insurance authorities designated by the National Association of Insurance Commissioners, and also with financial services industry, consumer organizations and privacy groups, and other representatives of the general public, in formulating and conducting the study required by subsection (a) of this section.

(c) Report

On or before January 1, 2002, the Secretary shall submit a report to the Congress containing the findings and conclusions of the study required under subsection (a) of this section, together with such recommendations for legislative or administrative action as may be appropriate.

(Pub. L. 106-102, title V, Sec. 508, Nov. 12, 1999, 113 Stat.1442.)

Sec. 6809. Definitions

As used in this subchapter:

(1) Federal banking agency

The term "Federal banking agency" has the same meaning as given in section 1813 of title 12.

(2) Federal functional regulator

The term ''Federal functional regulator'' means -

(A) the Board of Governors of the Federal Reserve System;

(B) the Office of the Comptroller of the Currency;

(C) the Board of Directors of the Federal Deposit Insurance Corporation;

(D) the Director of the Office of Thrift Supervision;

(E) the National Credit Union Administration Board; and

(F) the Securities and Exchange Commission.

(3) Financial institution

(A) In general

The term "financial institution" means any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12.

(B) Persons subject to CFTC regulation

Notwithstanding subparagraph (A), the term "financial institution" does not include 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.).

(C) Farm credit institutions

Notwithstanding subparagraph (A), the term "financial institution" does not include 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.).

(D) Other secondary market institutions

Notwithstanding subparagraph (A), the term "financial institution" does not include institutions chartered by Congress specifically to engage in transactions described in section 6802(e)(1)(C) of this title, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

(4) 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.

(5) Nonaffiliated third party

The term "nonaffiliated third party" means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution.

(6) Affiliate

The term ''affiliate'' means any company that controls, is controlled by, or is under common control with another company.

(7) Necessary to effect, administer, or enforce

The term "as necessary to effect, administer, or enforce the transaction" means -

(A) the disclosure is required, or is a usual, appropriate, or acceptable method, to carry out the transaction or the product or service business of which the transaction is a part, and record or service or maintain the

consumer's account in the ordinary course of providing the financial service or financial product, or to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part, and includes -

(i) providing the consumer or the consumer's agent or broker with a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product; and

(ii) the accrual or recognition of incentives or bonuses associated with the transaction that are provided by the financial institution or any other party;

(B) the disclosure is required, or is one of the lawful or appropriate methods, to enforce the rights of the financial institution or of other persons engaged in carrying out the financial transaction, or providing the product or service;

(C) the disclosure is required, or is a usual, appropriate, or acceptable method, for insurance underwriting 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; or

(D) the disclosure is required, or is a usual, appropriate or acceptable method, in connection with -

(i) 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;

(ii) the transfer of receivables, accounts or interests therein; or

(iii) the audit of debit, credit or other payment information.

(8) State insurance authority

The term "State insurance authority" means, in the case of any person engaged in providing insurance, the State insurance authority of the State in which the person is domiciled.

(9) Consumer

The term ''consumer'' means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.

(10) Joint agreement

The term ''joint agreement'' means a formal written contract pursuant to which two or more financial institutions jointly offer, endorse, or sponsor a financial product or service, and as may be further defined in the regulations prescribed under section 6804 of this title.

(11) Customer relationship

The term "time of establishing a customer relationship" shall be defined by the regulations prescribed under section 6804 of this title, and shall, in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services, mean the time of establishing the credit relationship withthe consumer.

(Pub. L. 106-102, title V, Sec. 509, Nov. 12, 1999, 113 Stat. 1443.)

REFERENCES IN TEXT

The Commodity Exchange Act, referred to in par. (3)(B), is act Sept. 21, 1922, ch. 369, 42 Stat. 998, as amended, which is classified generally to chapter 1 (Sec. 1 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see section 1 of Title 7 and Tables.

The Farm Credit Act of 1971, referred to in par. (3)(C), is Pub. L. 92-181, Dec. 10, 1971, 85 Stat. 583, as amended, which is classified generally to chapter 23 (Sec. 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

Sec. 6810. Effective Date

Pub. L. 106-102, title V, Sec. 510, Nov. 12, 1999, 113 Stat. 1445, provided that: "This subtitle (subtitle A (Sec. 501-510) of title V of Pub. L. 106-102, enacting this subchapter and amending section 1681s of this title) shall take effect 6 months after the date on which rules are required to be prescribed under section 504(a)(3) (15 U.S.C. 6804(a)(3)), except -

''(1) to the extent that a later date is specified in the rules prescribed under section 504; and

"(2) that sections 504 (15 U.S.C. 6804) and 506 (enacting section 6806 of this title and amending section 1681s of this title) shall be effective upon enactment (Nov. 12, 1999)."

FEDERAL TRADE COMMISSION

BUREAU OF CONSUMER PROTECTION
DIVISION OF FINANCIAL PRACTICES

The Gramm-Leach-Bliley Act
Privacy of Consumer Financial Information

Subtitle A of Title V of the Gramm-Leach-Bliley Act ("GLB Act") has privacy provisions relating to consumers' financial information. Under these provisions, financial institutions have restrictions on when they may disclose a consumer's personal financial information to nonaffiliated third parties. Financial institutions are required to provide notices to their customers about their information-collection and information-sharing practices. Consumers may decide to "opt out" if they do not want their information shared with nonaffiliated third parties. The GLB Act provides specific exceptions under which a financial institution may share customer information with a third party and the consumer may not opt out. All financial institutions are required to provide consumers with a notice and opt-out opportunity before they may disclose information to nonaffiliated third parties outside of what is permitted under the exceptions.

Subtitle A of Title V of the GLB Act and the Federal Trade Commission regulation can be found on the Gramm-Leach-Bliley Act web page which can be reached directly from the FTC home page at www.ftc.gov.

I. Important Dates and Citations about the Gramm-Leach-Bliley Act

Statute (Public Law 106-102, 15 U.S.C. § 6801, et seq.)
- enacted November 12, 1999

Regulations (16 C.F.R. § 313, 65 Fed. Reg. 33646 (May 24, 2000))
- effective date: November 13, 2000
- compliance date: July 1, 2001
- **Other Agencies' Rules**
  - Federal Reserve Board: 12 C.F.R. § 216
  - OTS: 12 C.F.R. § 573
  - OCC: 12 C.F.R. § 40
  - FDIC: 12 C.F.R. § 332
  - NCUA: 12 C.F.R. § 716
  - SEC: 17 C.F.R. § 248
  - CFTC: 17 C.F.R. § 160

** The views expressed in this presentation are not the official views of the Federal Trade Commission or of any individual Commissioner. June 18, 2001.*

II. Overview

A. Key Definitions
- Financial Institution
- Consumers and Customers
- Nonpublic Personal Information

B. Notices

C. Exceptions

D. Limits on Reuse and Redisclosure

III. Financial Institution

Definition: Any institution the business of which is engaging in *financial activities* as described in *section 4(k) of the Bank Holding Company Act* (12 U.S.C. § 1843(k)). Under the Final Rule promulgated by the Federal Trade Commission (FTC), an institution must be *significantly engaged* in financial activities to be considered a "financial institution."

A. Financial Activities:

- 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. [§ 4(k)(4)(A-E)]

- Engaging in an activity that the Federal Reserve Board has determined to be closely related to banking. [§ 4(k)(4)(F); 12 C.F.R. § 225.28]. 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. [§ 4(k)(4)(G); 12 C.F.R. § 211.5(d)]. For example:
  - Operating a travel agency in connection with financial services

- Only those activities determined to be financial activities under § 4(k)(1-3) as of November 12, 1999, are covered by the FTC Privacy Rule. While the Federal Reserve Board and the Department of Treasury have authority to add activities that are "incidental" or "complementary" to financial activities, the FTC will review those determinations before proposing to extend coverage of its Rule to such new activities.

B. Examples of businesses that engage in "financial activities" and are "financial institutions" for purposes of the GLB Act[1]:

- 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

C. "Significantly Engaged" in Financial Activities:

- 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 the GLB Act:
  - 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

[1] Even if a business engages in one of these financial activities, it does not necessarily have to provide privacy notices. The notice obligations depend on whether the business is providing a financial product or service to customers or, if they share the information with nonaffiliated third parties outside of specific exceptions, to consumers.

- 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 cars issued by others as its only means of extending credit

IV. Consumers and Customers

A. Consumers

Definition: A "consumer" is an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

Examples of Consumer Relationships:

- Applying for a loan
- Obtaining cash from a foreign ATM, even if it occurs on a regular basis
- Cashing a check with a check-cashing company
- Arranging for a wire transfer

General Obligations to Consumers:

- Provide an initial (or "short-form") notice about the availability of the privacy policy if the financial institution shares information outside the permitted exceptions.
- Provide an opt-out notice, with the initial notice or separately, prior to a financial institution sharing nonpublic personal information with nonaffiliated third parties.
- Provide consumers with a "reasonable opportunity" to opt out before disclosing nonpublic personal information about them to nonaffiliated third parties, such as 30 days from the date the notice is mailed.
    - If a consumer elects to opt out of all or certain disclosures, a financial institution must honor that opt-out direction as soon as is reasonably practicableafter the opt-out is received.
- If you change your privacy practices such that the most recent privacy notice you provided to a consumer is no longer accurate (e.g., you disclose a new category of NPI to a new nonaffiliated third party outside of specific exceptions and those changes are not adequately described in your prior notice), you must provide new revised privacy and opt-out notices.

B. Customers

Definition: A "customer" is a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship with a consumer.

Examples of Establishing a Customer Relationship:

- Opening a credit card account with a financial institution
- Entering into an automobile lease (on a non-operating basis for an initial lease term of at least 90 days) with an automobile dealer
- Providing personally identifiable financial information to a broker in order to obtain a mortgage loan
- Obtaining a loan from a mortgage lender
- Agreeing to obtain tax preparation or credit counseling services

"Special Rule" for Loans: The customer relationship travels with ownership of the servicing rights.

- A financial institution establishes a customer relationship with a consumer when it originates a loan.
- If it subsequently sells the loan and retains the servicing rights, it continues to have a customer relationship with the consumers.
- If it subsequently transfers the servicing rights, the entity that acquires servicing has a customer relationship with the consumer.
- Those with an ownership interest in the loan but without servicing rights have consumers.

General Obligations to Customers

- Provide an initial privacy notice not later than when the customer relationship is established.
- Provide, with the initial privacy notice or separately, an opt-out notice prior to sharing nonpublic personal information with nonaffiliated third parties outside of specific exceptions.
- Provide an annual privacy notice annually for the duration of the customer relationship.
- Provide customers with a "reasonable opportunity" to opt out before disclosing nonpublic personal information about them to nonaffiliated third parties, such as 30 days from the date the notice is mailed.
    - NOTE: If a customer elects to opt out of all or certain disclosures, a financial institution must honor that opt-out direction as soon as reasonably practicable after the opt-out is received.
- If you change your privacy practices such that the most recent privacy notice you provided to a consumer is no longer accurate (e.g., you disclose a new category of NPI or to a new nonaffiliated third party outside of specific exceptions and those changes are not adequately described in your prior notice), you must provide new revised privacy and opt-out notices.

V. Nonpublic Personal Information ("NPI")

NPI Includes:

- Nonpublic personally identifiable financial information; and

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

NPI Excludes:

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

"Personally Identifiable Financial Information" is any information:

- A consumer provides to obtain a financial product or service;
- About a consumer resulting from any transaction involving a financial product or service; or
- Otherwise obtained about a consumer in connection with providing a financial product or service.

"**Publicly Available Information" is:**

- Any information that a financial institution has a *reasonable basis to believe* is lawfully made available to the general public from:
  - Federal, State, or local government records;
  - Widely distributed media; or
  - Disclosures to the general public required by Federal, State, or local law.

"Reasonable Basis to Believe" means the financial institution:

- Cannot assume information is publicly available.
- Must take steps to determine if:
  - the information is of the type generally made available to the public;
  - whether an individual can direct that it not be made available; and
  - if so, whether that particular consumer has directed that it not be disclosed.

Examples of Publicly Available Information:

- Fact that an individual is a mortgage customer of a particular financial institution where that fact is recorded in public real estate records
- Telephone number listed in the phone book
- Information lawfully available to the general public on a website (including a website that requires a password or fee for access)

Examples of NPI (assuming such information is not publicly available):

- Fact that an individual is the customer of a particular financial institution
- Consumer's name, address, social security number, account number
- Any information a consumer provides on an application
- Information from a "cookie" obtained in using a website
- Information on a consumer report obtained by a financial institution (NOTE: Such information may also be covered by the Fair Credit Reporting Act)

NPI and Lists: Always consider how the list is derived.

- List of a finance company's mortgage customers with their outstanding mortgage balance and account numbers is NPI
- List of a retailer's credit card customers is NPI
- List of a retailer's credit card customers that is combined with a list of magazine subscribers is NPI
- List of all individuals who purchased washing machines from a retailer is NOT NPI where the information is not derived from information obtained in providing a financial product or service

VI. Notices

A. Types of Notices:

1. *Initial*: To customers not later than when relationship is established
   To consumers prior to sharing nonpublic personal information

2. *Opt-Out*: To consumers and customers prior to sharing information

3. *Short-Form*: To consumers who are not customers, in lieu of full initial notice, prior to sharing nonpublic personal information about them

4. *Simplified*: To customers if don't share NPI about current or former customers with affiliates or nonaffiliated third parties outside exceptions 313.14 and 313.15

5. *Annual*: To customers for duration of the relationship

6. *Revised*: To consumers, customers, and former customers

B. Format of Notices: Notices Must Be "Clear and Conspicuous"

1. "Clear and conspicuous" means that a notice must be reasonably understandable *and* designed to call attention to the nature and significance of the information in the notice.

2. "Reasonably understandable" means clear and concise sentences, plain language, active voice.

3. "Designed to call attention" means using headings, easily read typeface and type size, wide margins. On website: use text or visual cues to encourage scrolling down the page to view the entire notice; place notice on a frequently accessed page or via a clearly labeled link; ensure that there are no distracting graphics or sound.

C. Content of Initial and Annual Notices:
[for purposes of this section, "consumers" includes "customers"]

1. Categories of nonpublic personal information that the financial institution collects, for example:
   - information obtained from the consumer
   - information obtained from the consumer's transactions with a financial institution or its affiliate
   - information obtained from nonaffiliated third parties about the consumer's transactions with them
   - information obtained from a consumer reporting agency

2. Categories of nonpublic personal information that the financial institution discloses. Must provide illustrative examples, such as:
   - information from the consumer on applications or other forms, such as name, address, and social security number
   - information from transactions with the consumer: account number and balances, payment history, parties to transactions, credit card usage
   - information from a consumer reporting agency: creditworthiness and credit history

3. Categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information. Must provide illustrative examples, such as:
   - Financial service providers, such as mortgage brokers and insurance companies
   - Non-financial companies, such as magazine publishers, retailers, and direct marketers
   - Others, such as nonprofit organizations

4. If the financial institution discloses nonpublic personal information about former customers:
   - Categories of nonpublic personal information disclosed; and
   - Categories of affiliates and nonaffiliated third parties to whom nonpublic personal information is disclosed (other than what is permitted under exceptions 313.14 and 313.15).

5. If the financial institution discloses nonpublic personal information to a nonaffiliated third-party under exception 313.13 (for service providers and joint marketing partners):
   - Separate statement of the categories of nonpublic personal information disclosed (including illustrative examples); and
   - Statement about whether the third party is:
     - a service provider that performs marketing services on behalf of the financial institution itself or on behalf of products or services jointly marketed between two financial institutions; or
     - another financial institution with whom the financial institution has entered into a joint marketing agreement.

6. An explanation of the consumer's right to opt out.

7. Any disclosures that the financial institution is required to make under the Fair Credit Reporting Act.

8. The financial institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

9. If the financial institution discloses nonpublic personal information to a nonaffiliated third party under exceptions 313.14 and 313.15, state that disclosures to nonaffiliated third parties are made as permitted by law.

10. The financial institution may also reserve the right to disclose categories of nonpublic personal information that it does not currently disclose or categories of nonaffiliated third parties to which it does not currently disclose nonpublic personal information.

D. Content of Opt-out Notice

[for purposes of this section, "consumers" includes "customers"]

1. Fact that the financial institution discloses (or reserves the right to disclose) nonpublic personal information about a consumer to nonaffiliated third parties.
2. The consumer's right to opt out of those disclosures.
3. A description of a "reasonable means" by which the consumer can opt out, for example:
   - Toll-free telephone number
   - Detachable form with mailing information
   - If the consumer has agreed to receive notices electronically, an electronic means such as a form that can be sent via e-mail or through the financial institution's website

- NOTE: It is NOT a reasonable means to require a consumer to write her own letter as the ONLY option

Remember: A financial institution must allow a "reasonable opportunity" for the consumer to opt out before sharing information.

E. Content of the Short-Form Notice

1. State that the financial institution's full privacy policy is available on request.

2. Explain a reasonable means by which the consumer may obtain the full notice, for example:
   - Toll-free telephone number
   - On-site for in-person transactions

F. Content of Simplified Notice

1. List the categories of NPI collected.
2. Provide statement explaining that the institution does not share NPI with affiliates and nonaffiliated third parties, except as permitted by law (if applicable).
3. Provide statement explaining the institution's polices and practices with respect to safeguarding NPI.

G. Revised Notice

If a financial institution changes its policies and practices regarding disclosure of nonpublic personal information to nonaffiliated third parties outside of specific exceptions, it must:

- Provide a new notice that accurately reflects its policies; and
- Provide a new opt-out notice and a reasonable means to opt out.

H. Timing of Annual Notice

- Financial institution must provide an accurate privacy policy to its customers at least annually during the continuation of the customer relationship.

- Annually means at least once in a period of twelve consecutive months which the financial institution can define but must apply consistently. A financial institution can send annual notices to all its customers at the same time each year.
  - Customer opens account in January of 2004. Financial institution must send its first annual notice to that customer by December 2005.

I. Delivery of Notices

- Consumer or customer must be reasonably expected to receive actual notice in writing or, if the customer agrees, electronically. Examples of appropriate delivery include:
  - Hand delivery
  - Mail to last known address
  - For a consumer using an ATM, post the notice on the screen and require acknowledgment of receipt of the notice as a necessary part of the transaction.
  - For the consumer who conducts transactions electronically, post the notice on the website and require acknowledgment of receipt of the notice as a necessary part of the transaction.
  - For the customer who uses a website for electronic financial transactions and agrees to receive an annual notice at that website, post the current privacy notice continuously in a clear and conspicuous manner on that website.
  - The notice CANNOT just be posted in a branch or on a website.

- Customers must be provided notice in a form that can be retained or accessed at a later time.

VII. Exceptions

A financial institution may disclose nonpublic personal information to nonaffiliated third parties under several exceptions where consumers and customers do not have the right to opt out of such sharing and, in some cases, will get no notice of the disclosure.

A. Exception to Opt-Out Requirements: Section 313.13

- Financial institution must provide notice but not the right to opt out when it provides nonpublic personal information to:
  - Third party service provider that provides services for the financial institution; or
  - Other financial institution(s) with whom the financial institution has entered into a joint marketing agreement.

- Third party service provider may market the financial institution's own products and services or the financial products or services offered under a "joint marketing agreement" between the financial institution and one or more other financial institutions.

- Joint marketing agreement with other financial institution(s) means a written contract pursuant to which those institutions jointly offer, endorse, or sponsor a financial product or service.

- To take advantage of this exception the financial institution must:
  - Provide the initial notice as required to consumers and customers;

and

- Enter into a contract with the third party service provider or financial institution under a joint marketing agreement that prohibits the disclosure or use of the information other than for the purpose for which it was disclosed.

B. Exceptions to Notice and Opt-Out Requirements: Sections 313.14 and 313.15

Exception 313.14:

- Disclosures *necessary to effect, administer, or enforce a transaction* that a consumer requests or authorizes (see section 313.14(b)); or
- Disclosures made in connection with:
  - Servicing or processing a financial product or service that a consumer requests or authorizes
  - Maintaining or servicing a consumer's account
  - A proposed or actual securitization, secondary market sale (including the sale of servicing rights) or similar transactions

Exception 313.15:

- With consumer consent
- To protect the confidentiality or security of records
- To protect against or prevent actual or potential fraud
- For required institutional risk control or for resolving consumer disputes or inquires
- To persons holding a legal or beneficial interest relating to the consumer
- To persons acting in a fiduciary or representative capacity on behalf of the consumer (i.e., the consumer's attorney)
- To provide information to insurance rate advisory organizations, persons assessing compliance with industry standards, the financial institution's attorneys, accountants or auditors
- To law enforcement entities or self-regulatory groups (to the extent permitted or required by law)
- To comply with Federal, State, or local laws
- To comply with subpoena or other judicial process
- To respond to summons or other requests from authorized government authorities
- Pursuant to the Fair Credit Reporting Act, to a consumer reporting agency or from a consumer report reported by consumer reporting agency
- In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit

VIII. Limits on Reuse and Redisclosure by a Third Party

These restrictions apply to a third party that receives nonpublic personal information from a nonaffiliated financial institution.

A. Reuse and Redisclosure Under Exception 313.13: Information received under section 313.13 is restricted by the confidentiality agreement required under that section and cannot be used except for the purpose for which it was disclosed.

B. Reuse and Redisclosure Under Exceptions 313.14 and 313.15:
When a third party receives nonpublic personal information from a nonaffiliated financial institution under exception 313.14 or 313.15, the third party may:

- Disclose the information to affiliates of the financial institution from whom it received the information; or
- Disclose the information to its own affiliates who are limited in their use and disclosure of the information to the same extent as the third party; or
- Disclose and use the information pursuant to exceptions 313.14 or 313.15 in the ordinary course of business to carry out the activity covered by the exception for which it was received.

C. Reuse and Redisclosure Outside of Exceptions 313.14 and 313.15:
Where a third party receives nonpublic personal information from a financial institution outside of an exception (after the financial institution has provided notice and opt out and the consumer has not opted-out), the third party may:

- Disclose the information to the affiliates of the financial institution from whom it received the information; or
- Disclose the information to its own affiliates, who are limited in their use of information in the same manner as the third party; or
- Disclose the information to any other entity consistent with the privacy policy of the financial institution from which it received the information.

D. Examples of Limits on Reuse and Redisclosure:
A third party receives information from a financial institution to process account transactions authorized by consumers (pursuant to a section 313.14 exception):

- That third party may disclose that information to other nonaffiliated third parties in the ordinary course of business to carry out the servicing.
- It may also disclose it in response to a properly authorized subpoena.
- It *may not* use the information for its own marketing or sell it to another entity for marketing.

A magazine publisher purchases a list of a financial institution's customers (those who have not opted-out) where the disclosure falls outside the exceptions:

- It may use that list for its own purposes.
- It may disclose that list to other nonaffiliated third parties consistent with the financial institution's privacy policy.

IX. Other Issues

A. Prohibition on Sharing Account Numbers for Marketing Purposes

Financial institutions may not disclose, directly or through an affiliate, an account number of a consumer's credit card account, bank account, or transaction account to a nonaffiliated third party for use in marketing. A transaction account is an account to which a third party can initiate charges.

Exceptions:

- Disclosure to a consumer reporting agency.
- Disclosure to an agent or service provider to perform marketing of the financial institution's own products or services, provided that the agent or service provider is not authorized to directly initiate charges to the account.
- Disclosure to a participant in a private label credit card program or an affinity program where the participants are identified to the customer when the customer enters into the program.
- Disclosure of an encrypted account number to a nonaffiliated third party, provided that the financial institution does not give the third party the means to decode the number or code.

B. Effect on the Fair Credit Reporting Act

The FCRA is expressly not modified, limited, or superseded by Subtitle A of Title V of the GLB Act.

C. Relationship to State Laws:

State laws are not preempted except to the extent that they are "inconsistent" with this federal law. A state law is not "inconsistent" if it affords "greater protection" to consumers than provided for by this federal law, as determined by the FTC.

Hudson Cook, LLP
Attorneys at Law

2361 Rosecrans Avenue, Suite 355, El Segundo, California 90245
(310) 536-9099 • (800) 390-8288 • Fax: (310) 536-7644
www.hudco.com

Offices in: California, Connecticut, Maryland, New York, Virginia

January 14, 2003

Nathaniel Sterling, Executive Secretary
California Law Revision Commission
4000 Middlefield Road, Room D-1
Palo Alto, CA 94353-4739

Re: Study of Personal Information Relating to Financial Transactions

Dear Mr. Sterling:

Thank you for taking the time to speak with me in December about the California Law Revision Commission's upcoming meeting dedicated to the study of consumers' personal information relating to financial transactions.[1] The Consumer Financial Services Committee of the Business Law Section of The State Bar of California is very interested in this subject, and one or more Committee members will be attending the February 7, 2003 meeting in Sacramento.

As I mentioned during our telephone conversation, I thought it might be useful to supply a list of states that have enacted privacy legislation, or have legislation pending in the 2003 session, and although I am sure the Commissioners are aware of the federal laws and regulations that have been implemented dealing with financial privacy, a brief discussion precedes the state list, below. Reference to the local ordinances adopted in California is also included.

If you have any questions, or would like copies or more information about any of the items, please do not hesitate to let me know. I am looking forward to the February meeting.

Very truly yours,

Elizabeth A. Huber

Elizabeth A. Huber, Esq.
Chair, Consumer Financial Services Committee

Enclosures
cc: John Hancock, Financial Institutions Committee, Business Law Section
The State Bar of California: Saul Bercovitch, Larry Doyle, Susan Orloff

[1] Assembly Concurrent Resolution 125.

Summary of Federal Privacy Law Applicable to Financial Institutions: As you are aware, President Clinton signed the Gramm-Leach-Bliley Act into law[2] November 12, 1999. Subtitle A of Title V of the Gramm-Leach-Bliley Act (the "GLB Act")[3] limits the circumstances in which a "financial institution" may disclose nonpublic personal information about a consumer to a nonaffiliated third party. Among other things, Subtitle A of Title V of the GLB Act requires a financial institution to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with both affiliates and nonaffiliated third parties. The Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision ("Joint Agencies") released the implementing regulations[4] that became mandatory as of July 1, 2001, as did the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission.[5]

To implement the policy of safeguarding the security and confidentiality of the consumer nonpublic personal information required by the GLB Act, the Joint Agencies have also released the "Safeguards Rule,"[6] that is, the guidelines for establishing appropriate standards for the financial institutions subject to their respective jurisdictions relating to the administrative, technical and physical safeguards for customer records and information. The National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission[7] have also released Safeguards Rules.

Not long after the GLB Act was signed into law, state legislatures began to adopt state privacy laws. Throughout 2002, state legislatures continued to address not only privacy legislation, but also numerous other types of legislation that would protect consumers and their personal financial information, for example, identity theft legislation, social security number nondisclosure laws, online privacy laws, laws dealing with unsolicited telephone calls and "do not call" registries, and document/records destruction laws (these laws are not discussed in this letter). It is expected that in 2003, these concerns will continue to command the attention of the state legislators. Of states that have convened in 2003, the legislatures of California, New Hampshire, North Dakota and Texas have introduced privacy bills. New Jersey and Virginia each has legislation that is a "carried over" from 2002.

---

[2] Pub. L. 106-102.
[3] 15 U.S.C. §§ 6801 *et seq.*
[4] 65 Fed. Reg. 35162 (June 1, 2000).
[5] The Federal Trade Commission Privacy Rules are at 65 Fed. Reg. 33646 (May 24, 2000).
[6] 66 Fed. Reg. 8616 (February 1, 2001).
[7] The Federal Trade Commission Safeguards Rules are at 67 Fed. Reg. 36484 (May 23, 2002).

Enacted State Legislation Prior to 2002

Connecticut's Privacy Law: Effective July 1, 2001, House Bill 6132 (Public Act No. 01-76) (copy enclosed) requires a bank, Connecticut credit union, federal credit union, out-of-state bank with a branch in Connecticut, out-of-state trust company or out-of-state credit union that maintains an office in Connecticut, and all licensees under Title 36a of Connecticut General Statutes, including, for example, licensed mortgage lenders, mortgage loan brokers, small loan lenders, and sales finance companies, or any person subject to the jurisdiction of the Commissioner of Banking under Conn. Gen. Stat. Title 36b to comply with all applicable privacy requirements of Title V of the GLB Act, including implementing regulations, except to the extent that Connecticut's Deposit Account Privacy Statutes (Conn. Gen. Stats. §§ 36a-41 through 36a-44) provide greater consumer protections.

Georgia's Privacy Law: Georgia's privacy law pertains to sensitive information contained in public records. Senate Bill 205 (copy enclosed), signed April 2001, provides that Georgia's public records may not disclose a person's mother's birth name, credit card number, debit card number, bank account information and financial data or information.

Maine's Privacy Law: Maine's privacy law, Laws 2001 Ch. 262 (S.P. 521) (copy enclosed) effective September 1, 2001, took an interesting approach. Statutes regulating several types of financial institutions were amended to require that the entity regulated comply with the provisions of the GLB Act and implementing regulations

Missouri's Privacy Law: Missouri's privacy law became effective July 1, 2001. The law adopts federal GLB Act and gives authority to state agencies to adopt rules to carry out this law (a copy of House Bill 801 is enclosed).

North Dakota's Privacy Law: North Dakota's Disclosure of Customer Information Law, N.D. Cent. Code §§ 6-08.1-01 *et seq.*, was amended effective July 1, 2001, and repealed June 2002, by voter referendum. House Bill No. 1038 (copy enclosed) to be introduced in the current legislative session would again amend the state's privacy law.

Under the privacy law, a "financial institution" was not permitted to disclose customer information to any person, governmental agency, or law enforcement agency unless the disclosure was made within certain exceptions. A "financial institution" is defined as an organization authorized to do business under state or federal laws relating to financial institutions, including a bank, a savings bank, a trust company, a savings and loan association or a credit union.

The law did not apply to a disclosure of customer information by a financial institution to a nonaffiliated third party if the disclosure was subject to federal law on the date of the

disclosure, and the financial institution complied with applicable federal law in making the disclosure. The State Department of Financial Institutions had petitioned the Federal Trade Commission for a determination whether the law was preempted by federal law. The FTC responded June 28, 2001 (copy enclosed), indicating that the North Dakota law was not preempted.

In June 2002, North Dakota residents voted to repeal such amendments, which effectively reinstated the "opt-in" requirement for the sharing of nonpublic personal information by financial institutions. While the definition of "financial institution" appears to be broad, we understand that North Dakota regulators take the position that it applies to depository institutions, and not finance companies.

Tennessee's Privacy Law: Effective May 2001, the Tennessee legislature adopted the federal GLB Act (a copy of Senate Bill 1192 is enclosed).

Vermont's Privacy Law: Vermont's Privacy Law, Vt. Stat. Ann. §§ 10201 *et seq.*, was enacted in 1999. The regulations, adopted in 2001 by the Department of Banking, Insurance, Securities & Health Care Administration, are substantial. (Copies of both the statute and the regulations are enclosed).

Enacted State Legislation 2002

California Restrictions on "Display" of Social Security Number: A bill that was actually adopted in 2001, but effective July 1, 2002,[8] prohibits the public display of an individual's social security number by financial institutions and others, with some exceptions.[9]

California Local Ordinances: The following counties and cities have adopted privacy ordinances (copies enclosed): County of Alameda, Ord. No. 2003-28 effective September 1, 2003; County of Contra Costa, Ord. No. 2002-30 effective September 1, 2003; City of Daly City, Ord. No. 1295 effective January 1, 2003; City and County of San Francisco, Ord. No. 237-02 operative January 1, 2004; County of San Mateo, Ord. No. ____ effective January 1, 2003.

California Insurance Privacy Regulations: A copy of the Department of Insurance Privacy Regulations, 10 Cal. Code Regs. §§ 2689.1-2689.24, is enclosed.

Kentucky House Bill 79, Financial Information: With the passage of House Bill 79,[10] (copy enclosed), it is now a felony to attempt to or to improperly obtain financial information or to engage in the trafficking of financial information. The bill also creates unlawful circumstances under which the possession and use of the information is identity theft.

---

[8] Laws 2001, Ch. 720 (S.B. 168); Laws 2002, Ch. 1030 (A.B. 1068).
[9] *See* Cal. Civ. Code § 1798.85.
[10] Ky. Session Laws 2002, Ch. 175.

South Carolina Senate Bill 204, Family Privacy Protection Act (Public): Effective May 1, 2002, all state entities must develop privacy policies and procedures to ensure the collection of personal information pertaining to South Carolina citizens is limited to fulfill a legitimate purpose. As part of this legislation, any person or private entity is prohibited from obtaining or using any personal information from a public body for commercial solicitation directed at any person in South Carolina. A person who knowingly violates such prohibition is guilty of a misdemeanor, and upon conviction, must be fined an amount not to exceed $500 and/or imprisoned for a term not to exceed one year. (A copy of Senate Bill 204 is enclosed).

Washington Substitute House Bill 2015, Records Destruction: Washington enacted a new law, House Bill 2015 (copy enclosed), that requires entities (public and private alike) to take all reasonable steps to destroy, or arrange for the destruction of, personal financial and health information and personal identification numbers issued by government entities in an individual's records within its custody or control when the entity is disposing of records that it will no longer retain. The law provides that compliance with certain federal interagency guidelines establishing standards for safeguarding customer information is in compliance with the requirements of the law.

Proposed Legislation

California's Privacy Bills: Although California Senate Bill 773 (Speier) and Assembly Bill 1775 (Nation) had strong prospects of passage last year, the session adjourned without either bill having been passed. As is widely known, there are a number of bills introduced this year already dealing with privacy: Assembly Bill 7 (Corbett) and Assembly Bill 46 (Simitian) relating to identity theft; Senate Bill 1 (Speier and Burton) relating to privacy; Senate Bill 12 (Bowen) relating to electronic "spam"; Senate Bill 25 (Bowen) relating to consumer credit reporting; Senate Bill 27 (Figueroa) relating to disclosure to direct marketers; and Senate Bill 33 (Figueroa) relating to "do not call" lists.

As an interesting aside, with some exceptions, credit card issuers are already prohibited from releasing to marketers "marketing information" compiled by the card issuer based on a California cardholder's shopping patterns, spending history or behavioral characteristics derived from account activity without providing the cardholder notice and an opportunity to "opt out" of that sharing of information.[11] There is also an unusual provision in the California Public Utilities Code dealing with a customer's right to privacy, and a requirement that local telephone companies provide to residential customers information about state and federal laws that protect residential telephone subscriber's privacy rights.[12]

[11] Cal. Civ. Code § 1748.12.
[12] Cal. Pub. Ut. Code § 2894.10.

New Hampshire's Active Session: Among those 2003 legislative service requests (similar to the bill drafting process in California) are drafting requests for bills on financial privacy, personal information, social security number display restrictions, as well as limitations on access to public records for marketing purposes. The New Hampshire session is scheduled to open January 15, 2003. However, if you would like copies of these legislative service requests, please do not hesitate to let me know.

New Jersey Assembly Bill 2621 and Assembly Bill 1091, Opt-In Requirement for Nonaffiliated Third Party Information Sharing: These identical bills would prohibit "financial institutions" from disclosing to nonaffiliated third parties a customer's personal information without that customer's consent. Even with the customer's consent, the information that could be released would be limited to the customer's name, address, and telephone number. The bill contains GLB-type exceptions and, as it stands, only applies to state or federally chartered banks, savings banks, savings and loan association or credit unions, or any affiliate thereof.

New Jersey Senate Bill 1780, Financial Privacy: Introduced on September 12, 2002, Senate Bill 1780 would impose privacy policy notice requirements in addition to those required under the GLB Act. This bill would require a financial institution's privacy notice to contain the signal word "URGENT" at the top of the notice and mandate certain format opt-out requirements such as containing a box or space for the customer to mark as well as including a postage-paid return envelop and a toll-free number for inquiries.

Texas House Bill 56, Nondisclosure of Customer Information: A new chapter would be added to the Texas Finance Code that would require, with certain exceptions, a financial institution to obtain the customer's written consent before disclosing the customer's information to a nonaffiliated third party. The law would become effective September 1, 2003.

Virginia House Bill 866, Selling Personal Information Prohibited: This bill has seen no activity since its introduction in January 2002. The bill would add a provision to Virginia's Consumer Protection Act that would prohibit the sale of personal information gathered in connection with a consumer transaction from which judgments can be made about an individuals character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristic, including name, address and telephone number, to an entity not affiliated with a "supplier." A supplier is defined as a seller, lessor or licensor who advertises, solicits or engages in consumer transactions, or a manufacturer, distributor or licensor who advertises and sells, leases or licenses goods or services to be resold, leased or sublicensed by other persons in consumer transactions.

* * * * * *

SENATE BILL No. 1

Introduced by Senator Speier

December 2, 2002

An act to add Division 1.2 (commencing with Section 4050) to the Financial Code, relating to financial privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 1, as introduced, Speier. Financial institutions: nonpublic personal information.

Existing law provides for the regulation of banks, savings associations, credit unions, and industrial loan companies by the Department of Financial Institutions and by certain federal agencies. Existing federal law, the Gramm-Leach-Bliley Act, requires financial institutions to provide a notice to consumers relative to the use by the financial institution of nonpublic personal information, and in that regard authorizes consumers to direct that the information not be shared with nonaffiliated third parties.

This bill would enact the California Financial Information Privacy Act, which would require a financial institution, as defined, to provide a specified written form to a consumer relative to the sharing of the consumer's nonpublic personal information, as defined. The bill would allow a consumer to direct the financial institution to not share the nonpublic personal information with affiliated companies or with nonaffiliated financial companies with which the financial institution has contracted to provide financial products and services. The bill would require the permission of the consumer before the financial institution could share the nonpublic personal information with other nonaffiliated companies. The bill would provide that a financial institution is not required to provide this written form to its consumers

if the financial institution does not disclose any nonpublic personal information to any nonaffiliated 3rd party or to any affiliate.

This bill would provide that a financial institution shall not deny a consumer a financial product or service because the consumer has not provided the necessary consent that would authorize the financial institution to disclose or share nonpublic personal information. The bill would require a financial institution to comply with the consumer's request regarding nonpublic personal information within 45 days of receipt of the request.

This bill would provide that a financial institution may disclose nonpublic personal information to an affiliate or a nonaffiliated 3rd party in order for it to perform certain services on behalf of the financial institution if specified requirements are met. The bill would provide other exceptions from its provisions applicable to particular situations.

This bill would provide that nonpublic personal information may be released in order to identify or locate missing children, witnesses, criminals and fugitives, parties to lawsuits, and missing heirs and that it would not change existing law regarding access by law enforcement agencies to information held by financial institutions.

This bill would also provide for disclosure of nonpublic personal information under various other specified circumstances.

This bill would provide that enactment of these provisions preempts all local agency ordinances and regulations relating to this subject.

This bill would enact other related provisions.

This bill would also provide various civil penalties for negligent, or knowing and willful violations of these provisions. The penalties under the bill would not become operative until July 1, 2004.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Division 1.2 (commencing with Section 4050) is added to the Financial Code, to read:

DIVISION 1.2. CALIFORNIA FINANCIAL INFORMATION PRIVACY ACT

4050. This division shall be known and may be cited as the California Financial Information Privacy Act.

4051. (a) The Legislature intends for financial institutions to provide their consumers notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions.

(b) It is the intent of the Legislature in enacting the California Financial Information Privacy Act to afford persons greater privacy protection than those provided in Public Law 106–102, the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose.

4051.5. (a) The Legislature finds and declares all of the following:

(1) The California Constitution protects the privacy of California citizens from unwarranted intrusions into their private and personal lives.

(2) Federal banking legislation, known as the Gramm-Leach-Bliley Act, which breaks down restrictions on affiliation among different types of financial institutions, increases the likelihood that the personal financial information of California residents will be widely shared among companies.

(3) The policies intended to protect financial privacy imposed by the Gramm-Leach-Bliley Act are inadequate to meet the privacy concerns of California residents.

(4) Because of the limitations of these federal policies, the Gramm-Leach-Bliley Act explicitly permits states to enact privacy protections that are stronger than those provided in federal law.

(b) It is the intent of the Legislature in enacting this division:

(1) To ensure that Californians have the ability to control the disclosure of personally identifiable financial information for purposes other than those of the transactions into which they have entered.

(2) To achieve that control for California consumers by requiring that financial institutions that want to share information with third parties and unrelated companies seek and acquire the affirmative consent of California consumers.

(3) To further achieve that control for California consumers by providing consumers with the ability to prevent the sharing of financial information among affiliated companies through a simple opt-out mechanism.

(4) To provide a level playing field among types and sizes of businesses, including providing that those financial institutions with limited affiliate relationships may enter into agreements with other financial institutions on an ''affiliate-equivalent'' basis, as defined in statute, and providing that the different business models of differing financial institutions are treated in ways that provide consistent consumer control over information-sharing practices.

(5) To adopt to the maximum extent feasible, definitions consistent with federal law, so that in particular there is no change in the ability of businesses to carry out normal processes of commerce for transactions voluntarily entered into by consumers.

4052. For the purposes of this division:

(a) ''Nonpublic personal information'' means personally identifiable financial information (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution. Nonpublic personal information does not include publicly available information that the financial institution has a reasonable basis to believe is lawfully made available to the general public from (1) federal, state, or local government records, (2) widely distributed media, or (3) disclosures to the general public that are required to be made by federal, state, or local law. Nonpublic personal information 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 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.

(b) ''Personally identifiable financial information'' means information (1) that a consumer provides to a financial institution to obtain a product or service from the financial institution, (2) about a consumer resulting from any transaction involving a product or service between the financial institution and a consumer, or (3) that the financial institution otherwise obtains about a consumer in connection with providing a product or service to that consumer. Any personally identifiable information is financial if it was obtained by a financial institution in connection with providing a financial product or service to a

consumer, including the fact that a consumer is a customer of a financial institution or has obtained a financial product or service from a financial institution. Personally identifiable financial information includes all of the following:

(1) Information a consumer provides to a financial institution 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 consumer of a financial institution or has obtained a financial product or service from a financial institution.

(4) Any information about a financial institution's consumer if it is disclosed in a manner that indicates that the individual is or has been the financial institution's consumer.

(5) Any information that a consumer provides to a financial institution or that a financial institution or its agent otherwise obtains in connection with collecting on a loan or servicing a loan.

(6) Any personally identifiable financial information collected through an Internet cookie or an information collecting device from a Web server.

(7) Information from a consumer report.

(c) ''Financial institution'' means any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code and doing business in this state. An institution that is not significantly engaged in financial activities is not a financial institution. The term ''financial institution'' does not include the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. Sec. 2001 et seq.), provided that the entity does not sell or transfer nonpublic personal information to an affiliate or a nonaffiliated third party. 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.

(d) ''Affiliate'' means any entity that controls, is controlled by, or is under common control with, another entity, but does not include a joint employee of the entity and the affiliate. A

franchisor, including any affiliate thereof, shall be deemed an affiliate of the franchisee for purposes of this division. A financial institution and one or more of its affiliated entities shall be deemed a single entity for purposes of this division to the extent that (1) the financial institution and its affiliated entities are offering financial products or services in conjunction with and as part of a business that is significantly engaged in at least the following financial activities: (A) investment management services, (B) portfolio advisory services, and (C) financial planning, and (2) the operations of the financial institution and its affiliated entities are integrated and that integration facilitates the provision of those services.

(e) ''Nonaffiliated third party'' means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of that institution and a third party.

(f) ''Consumer'' means an individual resident of this state who obtains or has obtained a financial product or service from a financial institution, or that individual's legal representative. 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.

(g) ‘‘Control’’ means (1) ownership or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, acting through one or more persons, (2) control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, or (3) the power to exercise, directly or indirectly, a controlling influence over the management or policies of a company. However, for purposes of the application of the definition of control as it relates to credit unions, a credit union has a controlling influence over the management or policies of a credit union service organization (CUSO), as that term is defined by state or federal law or regulation, if the CUSO is at least 67 percent owned by credit unions. For purposes of the application of the definition of control to a financial institution subject to regulation by the United States Securities and Exchange Commission, a person who owns beneficially, either directly or through one or more controlled companies, more than 25 percent of the voting securities of a company is presumed to control the company, and a person who does not own more than 25 percent of the voting securities of a company is presumed not to control the company, and a presumption regarding control may be rebutted by evidence, but in the case of an investment company, the presumption shall continue until the United States Securities and Exchange Commission makes a decision to the contrary according to the procedures described in Section 2(a)(9) of the federal Investment Company Act of 1940.

(h) ‘‘Necessary to effect, administer, or enforce’’ means the following:

(1) The disclosure is required, or is a usual, appropriate, or acceptable method to carry out the transaction or the product or service business of which the transaction is a part, and record or service or maintain the consumer’s account in the ordinary course of providing the financial service or financial product, or to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part, and includes the following:

(A) Providing the consumer or the consumer’s agent or broker with a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product.

(B) The accrual or recognition of incentives or bonuses associated with the transaction or communications to eligible existing consumers of the financial institution regarding the availability of those incentives and bonuses that are provided by the financial institution or another party.

(2) The disclosure is required or is one of the lawful or appropriate methods to enforce the rights of the financial institution or of other persons engaged in carrying out the financial transaction or providing the product or service.

(3) The disclosure is required, or is a usual, appropriate, or acceptable method for insurance underwriting or the placement of insurance products by licensed agents and brokers with authorized insurance companies at the consumer's request, for reinsurance, stop loss insurance, or excess loss insurance purposes, or for any of the following purposes as they relate to a consumer's insurance:

(A) Account administration.

(B) Reporting, investigating, or preventing fraud or material misrepresentation.

(C) Processing premium payments.

(D) Processing insurance claims.

(E) Administering insurance benefits, including utilization review activities.

(F) Participating in research projects.

(G) As otherwise required or specifically permitted by federal or state law.

(4) The disclosure is required, or is a usual, appropriate, or acceptable method, in connection with the following:

(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.

(C) The audit of debit, credit, or other payment information.

(i) ''Financial product or service'' means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to a financial activity under subsection (k) of Section 1843 of Title 12 of the United States Code (the United States Bank Holding Company Act of 1956). Financial service includes a financial institution's

evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

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

(k) ''Widely distributed media'' means media available to the general public and includes 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.

4053. (a) A financial institution shall not disclose to, or share a consumer's nonpublic personal information with, any nonaffiliated third party, unless the financial institution has provided written notice pursuant to subdivision (c) to the consumer to whom the nonpublic personal information relates and unless the financial institution has obtained a consent acknowledgment from the consumer pursuant to subdivision (c) that authorizes the financial institution to disclose or share the nonpublic personal information. Nothing in this section shall prohibit the disclosure of nonpublic personal information as allowed in Section 4056. A financial institution shall not deny a consumer a financial product or a financial service because the consumer has not provided the consent required by this subdivision to authorize the financial institution to disclose or share his or her nonpublic personal information with any nonaffiliated third party. Nothing in this section is intended to prohibit a financial institution from offering incentives to elicit a specific response to the notice.

(b) (1) A financial institution shall not disclose to, or share a consumer's nonpublic personal information with, an affiliate unless the financial institution clearly and conspicuously notifies the consumer annually in writing pursuant to subdivision (c) that the nonpublic personal information may be disclosed to an affiliate of the financial institution and the consumer has not directed that the nonpublic personal information not be disclosed. A financial institution does not disclose information to, or share information with, its affiliate merely because information is maintained in common information systems or databases, and employees of the financial institution and its affiliate have access to those common information systems or databases, or a consumer accesses a Web

site jointly operated or maintained under a common name by or on behalf of the financial institution and its affiliate, provided that nonpublic personal information is used or otherwise disclosed only as permitted by this division.

(2) Subdivision (a) shall not prohibit the release of nonpublic personal information by a financial institution with whom the consumer has a relationship to a nonaffiliated financial institution for purposes of jointly offering a financial product or financial service pursuant to a written agreement with the financial institution that receives the nonpublic personal information provided that all of the following requirements are met:

(A) The financial product or service offered is a product or service of, and is provided by, at least one of the financial institutions that is a party to the written agreement.

(B) The financial product or service is jointly offered, endorsed, or sponsored, and clearly and conspicuously identifies for the consumer the financial institutions that release the nonpublic personal information and the financial institutions that receive that information.

(C) The written agreement provides that the financial institution that receives that nonpublic personal information is required to maintain the confidentiality of the information and is prohibited from disclosing or using the information other than to carry out the joint offering or servicing of a financial product or financial service that is the subject of the written agreement.

(D) The financial institution that releases the nonpublic personal information has complied with subdivision (c) and the consumer has not directed that the nonpublic personal information not be disclosed. The financial institution may, at its option, choose instead to comply with the requirements of subdivision (a).

(E) Notwithstanding this section, until January 1, 2005, a financial institution may disclose nonpublic personal information to a nonaffiliated financial institution pursuant to a preexisting contract with the nonaffiliated financial institution, for purposes of offering a financial product or financial service, if that contract was entered into on or before January 1, 2004. Beginning on January 1, 2005, no nonpublic personal information may be disclosed pursuant to that contract unless all the requirements of this subdivision are met.

(3) Nothing in this subdivision shall prohibit a financial institution from disclosing or sharing nonpublic personal information as otherwise specifically permitted by this division.

(c) (1) The form set forth in this subdivision or one substantially similar shall be sent by the financial institution to the consumer so that the consumer may make a decision and provide direction to the financial institution regarding the sharing of his or her nonpublic personal information. A form shall not be deemed substantially similar for purposes of this subdivision unless at least all of the following requirements are met:

(A) The form uses the same title (''IMPORTANT PRIVACY CHOICES FOR CALIFORNIANS'') and headers (headings designated in all capital letters in the form set forth below, such as ''SHARING INFORMATION WITH AFFILIATED COMPANIES'').

(B) The titles and headers in the form are clearly and conspicuously displayed, and no text in the form is smaller than 10-point type.

(C) The form is a separate document.

(2) (A) None of the instructional items appearing in parentheses in the form set forth below shall appear in the form provided to the consumer, as those items are for explanation purposes only. If a financial institution does not disclose or share nonpublic personal information as described in any one or more of the first three headers of the form, the financial institution is not required to include the applicable header or headers, and the accompanying information and box, in the form it provides pursuant to this subdivision.

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.

(B) If a consumer selects the box associated with the header restricting information sharing to the greatest extent allowed by law, that choice shall supersede all other choices.

(C) A financial institution shall not be in violation of this subdivision solely because it includes in the form one or more brief examples or explanations of the purpose or purposes, or context, within which information will be shared.

(D) The outside of the envelope in which the form is sent shall clearly state in 16-point boldface type ''IMPORTANT PRIVACY CHOICES,'' except that a financial institution sending the form to a consumer in the same envelope as a bill or account statement does not have to include the wording ''IMPORTANT PRIVACY CHOICES'' on that envelope. The form shall be sent in any of the following ways:

(i) With a bill or other statement of account, in which case the information required by Title V of the Gramm-Leach-Bliley Act may also be included.

(ii) As a separate notice or with the information required by Title V of the Gramm-Leach-Bliley Act, and including only information related to privacy.

(iii) With any other mailing, in which case it shall be the first page of the mailing.

(3) The consumer shall be provided an opportunity, before disclosure of information pursuant to this division, for 45 days from the date of postmark or other postal verification of mailing of the initial notice required by this subdivision, to direct that the nonpublic personal information not be disclosed except as otherwise permitted by this division. A consumer may direct at any time that his or her nonpublic personal information not be

disclosed, except as otherwise permitted by this division. A financial institution shall comply with a consumer's directions concerning the sharing of his or her nonpublic personal information within 45 days of receipt by the financial institution. When a consumer directs that nonpublic personal information not be disclosed, that direction is in effect until otherwise stated by the consumer.

(4) A financial institution shall not deny a consumer a financial product or a financial service because the consumer has directed pursuant to subdivision (b) that his or her nonpublic personal information not be disclosed provided that nothing in this section shall prohibit the disclosure of nonpublic personal information allowed by Section 4056. Nothing in this section is intended to prohibit a financial institution from offering incentives to elicit a specific response to the notice.

(5) A financial institution may elect to comply with the requirements of subdivision (a) with respect to disclosure of nonpublic personal information to an affiliate or with respect to nonpublic personal information disclosed pursuant to paragraph (2) of subdivision (b).

(6) If a financial institution does not have a continuing relationship with a consumer other than the initial transaction in which the product or service is provided, no annual disclosure requirement exists pursuant to this section as long as the financial institution provides the consumer with the form required by this section at the time of the initial transaction. As used in this section, ''annually'' means at least once in any period of 12 consecutive months during which that relationship exists. The financial institution may define the 12-consecutive-month period, but shall apply it to the consumer on a consistent basis. If, for example, a financial institution defines the 12-consecutive-month period as a calendar year and provides the annual notice to the consumer once in each calendar year, it complies with the requirement to send the notice annually.

(7) A financial institution with assets in excess of twenty-five million dollars ($25,000,000) shall include a self-addressed postage paid return envelope with the notice. A financial institution with assets of up to and including twenty-five million dollars ($25,000,000) shall include a self-addressed return envelope with the notice. In addition to the return envelope

required by this paragraph, a financial institution may offer additional means for consumers to communicate their privacy choices, including, but not limited to, calling a toll-free number, sending a facsimile, or using electronic means. A financial institution shall clearly and conspicuously disclose in the form required by this subdivision the information necessary to direct the consumer on how to communicate his or her choices, including the toll-free or facsimile number or Web site address that may be used, if those means of communication are offered by the financial institution.

(8) A financial institution shall file a copy of the initial notice or notices required by this subdivision with the Attorney General. No subsequent filing is required until the financial institution modifies the notice, in which case a copy of the notice as modified shall be filed with the Attorney General. Nothing in this paragraph shall be construed to require that a financial institution file with the Attorney General a copy of the notice or notices it provides to consumers more often than once in each calendar year. The interpretations of functional regulators regarding the form required by this subdivision are not entitled to deference by a court.

(d) Nothing in this division shall prohibit a financial institution from marketing its own products and services or the products and services of affiliates or nonaffiliated third parties to customers of the financial institution as long as (1) nonpublic personal information is not disclosed in connection with the delivery of the applicable marketing materials to those customers except as permitted by Section 4056 and (2) in cases in which the applicable nonaffiliated third party may extrapolate nonpublic personal information about the consumer responding to those marketing materials, the applicable nonaffiliated third party has signed a contract with the financial institution under the terms of which (A) the nonaffiliated third party is prohibited from retaining or using that information for any purpose, and (B) the financial institution has the right by audit, inspections, or other means to verify the nonaffiliated third party's compliance with that contract.

4053.5. Except as otherwise provided in this division, an entity that receives nonpublic personal information from a financial institution under this division shall not disclose this information to any other entity, unless the disclosure would be

lawful if made directly to the other entity by the financial institution. An entity that receives nonpublic personal information pursuant to any exception set forth in Section 4056 shall not use or disclose the information except in the ordinary course of business to carry out the activity covered by the exception under which the information was received.

4054. (a) Nothing in this division shall require a financial institution to provide a written notice to a consumer pursuant to Section 4053 if the financial institution does not disclose nonpublic personal information to any nonaffiliated third party or to any affiliate, except as allowed in this division.

(b) A notice provided to a member of a household pursuant to Section 4053 shall be considered notice to all members of that household unless that household contains another individual who also has a separate account with the financial institution.

(c) (1) The requirement to send a written notice to a consumer may be fulfilled by electronic means if the following requirements are met:

(A) The notice, and the manner in which it is sent, meets all of the requirements for notices that are required by law to be in writing, as set forth in Section 101 of the federal Electronic Signatures in Global and National Commerce Act.

(B) All other requirements applicable to the notice, as set forth in this division, are met, including but not limited to, requirements concerning content, timing, form, and delivery.

(C) The notice is delivered to the consumer in a form the consumer may keep.

(2) A notice that is made available to a consumer, and is not delivered to the consumer, does not satisfy the requirements of paragraph (1).

(3) Any electronic consumer reply to an electronic notice sent pursuant to this division is effective. A person that electronically sends a notice required by this division to a consumer may not by contract, or otherwise, eliminate the effectiveness of the consumer's electronic reply.

(4) This division modifies the provisions of Section 101 of the federal Electronic Signatures in Global and National Commerce Act. However, it does not modify, limit, or supersede the provisions of subsection (c), (d), (e), (f), or (h) of Section 101 of the federal Electronic Signatures in Global and National

Commerce Act, nor does it authorize electronic delivery of any notice of the type described in subsection (b) of Section 103 of that federal act.

4054.6. When a financial institution and a membership organization, tax-exempt organization, not-for-profit organization, or a professional sports team that is not a financial institution have an agreement to issue a credit card in the name of the membership organization, tax-exempt organization, not-for-profit organization, or the professional sports team (‘‘affinity card’’), the financial institution shall be permitted to disclose to the entity in whose name the card is issued, the names and addresses, including electronic mail addresses, of the financial institution’s consumers in receipt of the affinity card if all of the following requirements are satisfied:

(a) The financial institution has provided the notice required by this division to the consumer, and the consumer has not directed that confidential consumer information not be disclosed.

(b) The financial institution has a contractual agreement with the membership organization, tax-exempt organization, not-for-profit organization, or professional sports team that requires the entity in whose name the affinity card is issued to maintain the confidentiality of the nonpublic personal information and prohibits the entity in whose name the affinity card is issued from using the information for any purposes other than verifying membership, verifying the affinity cardholder’s address, or offering the entity’s own products or services to the cardholder. Nothing in this section shall prohibit the disclosure of nonpublic personal information allowed by Section 4056.

(c) The customer list is not disclosed in any way that reveals or permits extrapolation of any additional nonpublic personal information about any customer on the list.

(d) If the entity in whose name the card is issued sends any message to any electronic mail addresses obtained pursuant to this section, the message shall include at least both of the following:

(1) The identity of the sender of the message.

(2) A cost-free means for the recipient to notify the sender not to electronically mail any further messages to the recipient.

4056. (a) This division shall not apply to information that is not personally identifiable to a particular person.

(b) Sections 4053 and 4054 shall not prohibit the release of nonpublic personal information under the following circumstances:

(1) The nonpublic personal information is necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with servicing or processing a financial product or service requested or authorized by the consumer, or in connection with 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 that entity, or in connection with a proposed or actual securitization or secondary market sale, including sales of servicing rights, or similar transactions related to a transaction of the consumer.

(2) The nonpublic personal information is released with the consent of or at the direction of the consumer.

(3) The nonpublic personal information is:

(A) Released 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) Released to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability.

(C) Released for required institutional risk control, or for resolving customer disputes or inquiries.

(D) Released to persons holding a legal or beneficial interest relating to the consumer, including for purposes of debt collection.

(E) Released to persons acting in a fiduciary or representative capacity on behalf of the consumer.

(4) The nonpublic personal information is released 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) The nonpublic personal information is released to the extent specifically required or specifically permitted under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. Sec. 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. Secs. 1951-1959), the California Department of Insurance or other state insurance regulators, or the Federal Trade Commission, and self-regulatory organizations, or for an investigation on a matter related to public safety.

(6) The nonpublic personal information is released 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 the business or unit.

(7) The nonpublic personal information is released to comply with federal, state, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, administrative, 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.

(8) 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 pursuant to Article 3 (commencing with Section 15630) of Chapter 11 of Part 3 of Division 9 of the Welfare and Institutions Code.

(9) The nonpublic personal information is released to an affiliate or a nonaffiliated third party in order for the affiliate or nonaffiliated third party to perform services, such as mailing services, data processing or analysis, or customer surveys, on behalf of the financial institution, provided that all of the following requirements are met:

(A) The services to be performed by the affiliate or nonaffiliated third party could lawfully be performed by the financial institution.

(B) There is a written contract between the affiliate or nonaffiliated third party and the financial institution that prohibits the affiliate or nonaffiliated third party, as the case may be, from disclosing or using the nonpublic personal information other than

to carry out the purpose for which the financial institution disclosed the information, as set forth in the written contract.

(C) The nonpublic personal information provided to the affiliate or nonaffiliated third party is limited to that which is reasonably necessary for the affiliate or nonaffiliated third party to perform the services contracted for on behalf of the financial institution.

(D) The financial institution does not receive any payment from or through the affiliate or nonaffiliated third party in connection with, or as a result of, the release of the nonpublic personal information.

(10) 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.

(11) 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.

(12) The nonpublic personal information is released as required by Title III of the federal United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act; P.L. 107-56).

(c) Nothing in this division is intended to change existing law relating to access by law enforcement agencies to information held by financial institutions.

4056.5. (a) The provisions of this division do not apply to any person or entity that meets the requirements of paragraph (1) or (2) below. However, when nonpublic personal information is being or will be shared by a person or entity meeting the requirements of paragraph (1) or (2) with an affiliate or nonaffiliated third party, this division shall apply.

(1) The person or entity is licensed in one or both of the following categories and is acting within the scope of the respective license or certificate:

(A) As an insurance producer, licensed pursuant to Chapter 5 (commencing with Section 1621), Chapter 6 (commencing with Section 1760), or Chapter 8 (commencing with Section 1831) of Division 1 of the Insurance Code, as a registered investment adviser pursuant to Chapter 3 (commencing with Section 25230) of Part 3 of Division 1 of Title 4 of the Corporations Code, or as an investment adviser pursuant to Section 202(a)(11) of the federal Investment Advisers Act of 1940.

(B) Is licensed to sell securities by the National Association of Securities Dealers (NASD).

(2) The person or entity meets the requirements in paragraph (1) and has a written contractual agreement with another person or entity described in paragraph (1) and the contract clearly and explicitly includes the following:

(A) The rights and obligations between the licensees arising out of the business relationship relating to insurance or securities transactions.

(B) An explicit limitation on the use of nonpublic personal information about a consumer to transactions authorized by the contract and permitted pursuant to this division.

(C) A requirement that transactions specified in the contract fall within the scope of activities permitted by the licenses of the parties.

(b) The restrictions on disclosure and use of nonpublic personal information, and the requirement for notification and disclosure provided in this division, shall not limit the ability of insurance producers and brokers to respond to written or electronic, including telephone, requests from consumers seeking price quotes on insurance products and services or to obtain competitive quotes to renew an existing insurance contract, provided that any nonpublic personal information disclosed pursuant to this subdivision shall not be used or disclosed except in the ordinary course of business in order to obtain those quotes.

4057. (a) An entity that negligently discloses or shares nonpublic personal information in violation of this division shall be liable, irrespective of the amount of damages suffered by the consumer as a result of that violation, for a civil penalty not to exceed two thousand five hundred dollars ($2,500) per violation. However, the total civil penalty awarded pursuant to this

subdivision shall not exceed five hundred thousand dollars ($500,000) per occurrence.

(b) An entity that knowingly and willfully obtains, discloses, shares, or uses nonpublic personal information in violation of this division shall be liable for a civil penalty not to exceed two thousand five hundred dollars ($2,500) per violation.

(c) 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.

(d) In the event a violation of this division results in the identity theft of a consumer, as defined by Section 530.5 of the Penal Code, the civil penalties set forth in this section shall be doubled.

(e) This section shall become operative on and after July 1, 2004, for acts in violation of this division that occur on and after July 1, 2004.

4058. Nothing in this division shall be construed as altering or annulling the authority of any department or agency of the state to regulate any financial institution subject to its jurisdiction.

4058.5. This division shall preempt and be exclusive of all local agency ordinances and regulations relating to the use and sharing of nonpublic personal information by financial institutions. This section shall apply both prospectively and retroactively.

4059. The provisions of this division shall be severable, and if any phrase, clause, sentence, or provision is declared to be invalid or is preempted by federal law or regulation, the validity of the remainder of this division shall not be affected thereby.

O