SCHWARTZ & BALLEN LLP
1990 M STREET, N.W. · SUITE 500
WASHINGTON, DC 20036-3465

(202) 776-0700

FACSIMILE
(202) 776-0720

M E M O R A N D U M

September 18, 2003

Re: California Financial Information Privacy Act (SB 1)

INTRODUCTION

The State of California recently enacted the Financial Information Privacy Act (the "Act"),[1] which imposes requirements on disclosures by financial institutions that do business with California residents that are more restrictive than those set forth in Title V of the Gramm-Leach-Bliley Act. The Act affects the ability of financial institutions to disclose information about customers to affiliates as well as nonaffiliates. The provisions of the Act become effective on July 1, 2004.[2]

Subject to certain exceptions, a financial institution generally may not disclose nonpublic personal information of a consumer to a nonaffiliated third party that is not a financial institution unless it obtains the consumer's explicit prior consent.[3] A financial institution may not disclose nonpublic personal information of a consumer to an affiliate unless it clearly and conspicuously notifies the consumer annually that the information may be disclosed to an affiliate and the consumer has not directed that the information not be disclosed.[4] A financial institution may disclose nonpublic personal information of a consumer to a nonaffiliated financial institution with which it has a joint marketing agreement if it uses the form prescribed in the Act to notify the consumer that the information may be disclosed and the consumer has not directed that the information not be disclosed.[5] A financial institution may, however, disclose information about its customers for operational purposes and under certain other circumstances as set forth below.[6]

---

[1] California Financial Information Privacy Act, S.B. 1, 2003-2004 Leg., Reg. Sess. (Cal. 2003) (approved August 27, 2003).
[2] § 4060.
[3] § 4052.5; § 4053(a)(1).
[4] § 4053(b)(1).
[5] § 4053(b)(2).
[6] § 4056.

DEFINITIONS

Nonpublic Personal Information

"Nonpublic personal information" is personally identifiable financial information (1) provided by a consumer to a financial institution; (2) resulting from a transaction between the financial institution and the consumer; or (3) otherwise obtained by the financial institution.[7] Nonpublic personal information includes any list, description or other grouping of consumers, and publicly available information about them, that is derived using nonpublic personal information.

Personally Identifiable Financial Information

"Personally identifiable financial information" means information (1) provided by a consumer to obtain a product or service; (2) about a consumer resulting from a transaction with a consumer involving a product or service; or (3) that the institution otherwise obtains while providing a product or service to a consumer.[8] Personally identifiable information is considered financial if the institution obtained it in connection with providing a financial product or service to a consumer.[9]

The following are regarded as personally identifiable financial information: (1) information provided by a consumer in an application for a financial product or service, such as a credit card or loan; (2) account balance, payment history, overdraft history, and credit or debit card information; (3) the fact that the institution has or had a relationship with the consumer; (4) information regarding a consumer if it is disclosed in such a way as to indicate the individual is or has been the financial institution's consumer; (5) any information the consumer provides to the financial institution, or that it or its agent collects in the course of collecting or servicing a loan; (6) information collected through use of Internet cookies or devices on a web server; and (7) information from a consumer report.[10]

Financial Institution

A financial institution means any institution that significantly engages in financial activities, as described in the Bank Holding Company Act, as amended by the Gramm-Leach-Bliley Act, and is doing business in California.[11]

---

[7] § 4052(a).
[8] § 4052(b).
[9] *Id*.
[10] *Id*.
[11] § 4052(c).

Financial Product or Service

A financial product or service is one that a financial holding company may offer by engaging in an activity that is financial in nature or incidental to a financial activity under the Bank Holding Company Act.[12] The term also includes a financial institution's evaluation or brokerage of information the institution collects in connection with a request or application by a consumer for a financial product or service.[13]

Affiliate

An affiliate is any entity that controls, is controlled by, or is under common control with, another entity, but does not include a joint employee.[14] A franchisor is considered an affiliate of the franchisee.[15]

Nonaffiliated Third Party

A nonaffiliated third party is an entity that is not an affiliate of the financial institution.[16] A nonaffiliated third party does not include a joint employee.[17]

Consumer

A consumer is a resident of California who obtains, or has obtained, a financial product or service from a financial institution primarily for personal, family or household purposes.[18] A person is a resident of California if the person's last known mailing address (as reflected in the institution's records) is California. A person is not a consumer simply by participating in (1) an employee benefit plan; (2) a group insurance policy or annuity contract; or (3) a workers' compensation plan, or by being the beneficiary of a trust administered by the financial institution, or by designating the financial institution as trustee of a trust if the financial institution has provided the required notices to the plan sponsor or group policyholder.[19]

---

[12] 12 U.S.C. 1843(k).
[13] S.B. 1 § 4052(i).
[14] § 4052 (d).
[15] *Id*.
[16] § 4052(e).
[17] *Id*.
[18] § 4052 (f).
[19] *Id*.

DISCLOSURES

Disclosures to Nonaffiliated Third Parties

The Act requires that a financial institution obtain a consumer's explicit consent (*i.e.*, opt-in) prior to disclosing the consumer's nonpublic personal information to a nonaffiliated third party.[20] Exceptions to this general restriction are provided for disclosures that are necessary to deliver the product or service requested and for certain other operating reasons. In addition, as indicated below, the requirement of prior consent does not apply to disclosures to other financial institutions with which the institution has a joint marketing agreement.

The consumer's consent must be in writing, in a separate document, dated and signed by the consumer.[21] The form must clearly and conspicuously state that, upon signing, the consumer consents to disclosure of nonpublic personal information to nonaffiliated third parties.[22] Additionally, the consent form must state (1) that the consent remains effective until the consumer revokes or modifies the consent; (2) that the consumer may do so at any time; and (3) the procedure to be used by the consumer to revoke the consent.[23] Finally, the form must state that the financial institution will retain the consent or a copy, indicate that the consumer may want to retain a copy, and explain that the consumer is entitled to a copy from the institution upon request.[24]

Joint Agreements

A financial institution may, without consent, disclose a consumer's nonpublic personal information to a nonaffiliated financial institution for purposes of jointly offering a financial product or service pursuant to a written agreement, as long as the consumer has been provided an opportunity to direct the financial institution not to share information about the consumer with other institutions (*i.e.*, opt-out) and the consumer has not opted-out from such disclosures.[25] Until January 1, 2005, however, a financial institution may disclose nonpublic personal information to a nonaffiliated financial institution pursuant to a preexisting contract, without giving the consumer an opportunity to opt-out, if that contract had been entered into on or before January 1, 2004.[26]

Disclosures to Affiliates

The Act provides that a financial institution may not disclose a consumer's nonpublic personal information to an affiliate unless it has notified the consumer annually

---

[20] § 4052.5.
[21] § 4053(a)(2).
[22] § 4053(a)(2)(C).
[23] § 4053(a)(2)(D).
[24] § 4053(a)(2)(E).
[25] § 4053(b)(2).
[26] § 4053(b)(2)(E).

in writing that the information may be disclosed to an affiliate and the consumer has not informed the institution not to disclose the information to its affiliate (*i.e.*, the consumer has not opted out).[27] Financial institutions may, in the alternative, choose to comply with the consent form requirements applicable to nonaffiliated third parties.[28]

A financial institution does not disclose information to an affiliate merely because information is maintained in a common database to which the affiliate has access, provided that if a consumer has exercised his or her opt-out option, such information is not further disclosed or used by the affiliate.[29] In addition, a financial institution is not prohibited from sharing nonpublic personal information with a financial institution affiliate[30] if the two institutions are regulated by the same functional regulator,[31] are engaged in the same line of business,[32] and share a common brand which is used to identify the source of the products and services provided.[33] The Act permits institutions to offer incentives or discounts to encourage consumers to respond to notices.[34]

Nondiscrimination

A financial institution may not discriminate against or deny an otherwise qualified consumer a product or service because the consumer has not provided his or her consent to disclose the consumer's nonpublic personal information to nonaffiliated third parties[35] or has directed that the consumer's nonpublic personal information not be disclosed to affiliates.[36] However, this does not prevent a financial institution from denying a product or service if it could not provide it without the consumer's consent to disclose information and the consumer has failed to provide consent.[37]

---

[27] § 4053(b)(1).
[28] § 4053(b)(5).
[29] § 4053(b)(1).
[30] To fall under this provision, the Act requires that the financial institution affiliates must be wholly owned. § 4053(c).
[31] Institutions regulated by any federal and state depository institution supervisor are regarded as being regulated by the same functional regulator. Institutions regulated by the Securities and Exchange Commission, the U.S. Department of Labor or a state securities regulator are regarded as being regulated by the same functional regulator. Insurers licensed in California are deemed to be in compliance with the provision as well.
[32] A line of business is one of the following: insurance, banking or securities.
[33] § 4053(c).
[34] § 4053(a)(1), (b)(4).
[35] § 4053(a)(1),
[36] § 4053(b)(4).
[37] § 4053(a)(1), (b)(4).

OTHER PROVISIONS

Forms

The Act provides a model form that financial institutions may use to satisfy the notice requirements before sharing information with affiliates and companies with which the financial institution contracts to provide financial products and services to the consumer. Use of the model form provides a safe harbor for financial institutions and constitutes a conclusive presumption of compliance with the notice requirements of the Act.[38] If an institution does not use the model form, the Act sets out numerous requirements that must be met, including that the notice form be one page, no text be smaller than 10-point type and that the form achieve a minimum Flesch reading ease score of 50.[39] A financial institution may submit its alternative form to its functional regulator for approval, and for a form filed with the California Office of Privacy Protection before July 1, 2007, the approval constitutes a rebuttable presumption that the form complies with the Act.[40] The financial institution and its affiliates or other financial institutions identified in the notice may send a joint notice to consumers.[41]

The notice must be sent in an envelope that contains the following wording in 16-point boldface type: "IMPORTANT PRIVACY CHOICES."[42] However, if the notice is sent with a bill, an account statement or an application requested by the consumer, no notice need appear on the envelope.[43] If the model notice is not used, the financial institution must file the notice it uses with the Office of Privacy protection within 30 days of first using it.[44]

A financial institution with assets over $25 million must include a self-addressed business reply envelope with the notice.[45] As an alternative, a financial institution with assets over $25 million may include a self-addressed return envelope (*i.e.*, not a business reply) and two alternative cost-free means for consumers to exercise their options (*e.g.*, toll-free number, facsimile or electronic means).[46]

Waiting Periods

A financial institution must provide a reasonable opportunity prior to disclosure for a consumer to direct the institution not to disclose the consumer's information.[47] The institution must then comply with the consumer's direction within 45 days of receiving

---

[38] § 4053(d)(1).
[39] *Id*.
[40] § 4053(d)(2)(B).
[41] § 4053(d)(7).
[42] § 4053(d)(2)(D).
[43] *Id*.
[44] § 4053(d)(2)(E).
[45] § 4053(d)(6).
[46] *Id*.
[47] § 4053(d)(3).

the request. A consumer can at any time direct that his or her information not be shared, and the consumer's request will remain in effect until the consumer otherwise notifies the institution.[48]

If the institution has not previously provided an annual opt-out form to the consumer pursuant to the provision of the Act regarding disclosure to affiliates, it shall provide a form and wait 45 days before disclosing the consumer's nonpublic personal information.[49] If a financial institution does not have a continuing relationship with the consumer, no annual disclosure need be made.[50]

Marketing of the Financial Institution's Products and Services

A financial institution may market its own products and services or those of affiliates or nonaffiliates to its customers.[51] In so doing, the institution cannot disclose nonpublic personal information unless permitted under an operational exception,[52] as explained below. If a nonaffiliated third party could extrapolate nonpublic personal information from the consumer's response to marketing materials, it must agree in writing that it will not use the information for any purpose other than the purpose for which it was provided, and the financial institution must be permitted to verify compliance.[53]

Mode of Notice

Required notices may be in electronic form if they comply with the Electronic Signatures in Global and National Commerce (E-Sign) Act in substance and the manner in which they are sent, and with the requirements of the Act (*e.g.*, content, timing, form, and delivery).[54] The electronic notice must be delivered to the consumer and be in a form the consumer can retain as a record.[55] Electronic consumer replies to electronic notices are also permitted.[56] Notice sent to one member of a household is deemed notice to all members, unless another member has a separate account at the financial institution.[57]

Affinity Programs

Financial institutions that offer credit cards in the names of non-financial institution partners (an "affinity card") may disclose only their customers' names, addresses, telephone numbers, electronic mail addresses and records of purchases made

---

[48] *Id.*
[49] *Id.*
[50] § 4053(d)(5).
[51] § 4053(e).
[52] *See* § 4056.
[53] § 4053(e).
[54] § 4054(c)(1).
[55] *Id.*
[56] *Id.*
[57] § 4054(b).

using the affinity card to the affinity partner.[58] If a financial institution provides financial services or products other than credit cards on behalf of an affinity partner, the institution may disclose only the names, addresses, telephone numbers, and electronic mail addresses of customers who obtained the product or service.[59]

Disclosure to affinity partners is permitted only if the financial institution sent a notice to the consumer and the consumer did not opt-out.[60] The affinity partner must also agree in writing to maintain the confidentiality of the nonpublic personal information and to use it only to verify the consumer's membership or contact information or to offer its own products or services.[61] The affinity partner must identify itself in any electronic mail message to the consumer and provide a cost-free mechanism for the consumer to be taken off the electronic mail list.[62]

Operational Exceptions

The Act contains exceptions to the restrictions on disclosure for operational purposes.[63] The financial institution may disclose information as necessary to enforce its lawful rights in carrying out the transaction[64] or, on behalf of the consumer, for insurance purposes.[65] The operational exceptions are essentially identical to those provided in the Gramm-Leach-Bliley Act.

For example, a financial institution may disclose nonpublic personal information if necessary to effect, administer or enforce a transaction requested or authorized by a consumer; to protect the confidentiality or security of the institution's records; to protect against fraud, theft, claims, institutional risk or other liabilities; to assist persons representing the consumer in a legal, fiduciary or representative capacity; or to assist in law enforcement or regulatory compliance.[66] An entity that receives nonpublic personal information pursuant to an exception may not use or disclose it except to carry out the activity covered by the exception under which the information was received.[67]

The Act also provides an exception for disclosures to licensed insurance producers and persons licensed by the National Association of Securities Dealers ("NASD") to sell securities.[68] However, such persons are subject to the provisions of the Act if they wish to disclose information to affiliated or nonaffiliated third parties.[69] A contract between licensed insurance producers or NASD licensed sellers of securities and

[58] § 4054.6(a).
[59] § 4054.6(b).
[60] § 4054.6(c).
[61] *Id*.
[62] *Id*.
[63] § 4056(b).
[64] § 4052 (h)(2).
[65] § 4052 (h)(3).
[66] § 4056(b)(1).
[67] § 4053.5.
[68] § 4056.5.
[69] *Id*.

other persons or entities will be excepted from the Act if the contract specifies the rights and obligations of the licensees of the parties with respect to the transaction, explicitly limits the use of nonpublic personal information in the transaction, and requires that the transaction be within the scope of activities permitted by licensees of the parties.[70]

The Act does not restrict the ability of insurance producers and brokers to respond to requests for price quotes or their ability to seek competitive quotes, as long as any disclosed nonpublic personal information is disclosed in the ordinary course of business to obtain the quotes.[71] Disclosure by an insurer or affiliate to its exclusive agent is permitted, though the agent may not then disclose the information except as permitted by the Act.[72] An insurer or affiliate does not disclose information to an exclusive agent merely because it is maintained in a common database, provided that if a consumer has exercised his or her opt-out option, the information is not further disclosed or used by the exclusive agent for other purposes.[73]

Penalties

An entity that negligently discloses nonpublic personal information in violation of the Act is liable for a civil penalty of up to $2,500 per violation.[74] If the violation resulting from the disclosure of information relates to more than one consumer, the entity is subject to a maximum penalty of up to $500,000.[75] A person who knowingly and willfully obtains, discloses, shares or uses information in violation of the Act is subject to a civil penalty of up to $2,500 per individual violation.[76] If a violation of the Act results in identity theft, the Act provides for double civil penalties.[77] The penalties may be imposed regardless of whether or not the consumer incurred damages as a result of the violation.[78]

In determining the penalty for violations, the Act provides that courts should consider the following factors: (1) total assets and net worth of the violating entity; (2) nature and seriousness of the violation; (3) persistence of the violation and any attempts to correct it; (4) length of time over which the violation occurred; (5) number of times the entity violated the Act; (6) harm to consumers; (7) proceeds derived from the violation; and (8) the impact of potential penalties on the solvency of the entity.[79]

---

[70] *Id*.
[71] § 4056.5(b).
[72] § 4056.5(c)(1).
[73] *Id*.
[74] § 4057(a).
[75] *Id*.
[76] § 4057(b).
[77] § 4057(d).
[78] § 4057(a), (b).
[79] § 4057(c).

Enforcement actions may be brought by the Attorney General of California and by the institution's federal or state functional regulator.[80]

Preemption

The Act prospectively and retroactively preempts all local California ordinances and regulations relating to the disclosure of nonpublic personal information by financial institutions.[81] However, it does not preempt the authority of a California department or agency to regulate any financial institution subject to its jurisdiction.[82]

[80] § 4057(e).
[81] § 4058.5
[82] § 4058.