SB-1: The California Financial Information Privacy Act—Interim and Permanent Compliance Considerations

Introduction

On July 30, 2004, the U.S. District Court for the Eastern District of California ruled that the FACT Act and the FCRA did not preempt the California Financial Information Privacy Act (commonly referred to as “SB-1”), and refused to enjoin enforcement of SB-1’s July 1, 2004 effective date. The plaintiff bank trade groups have appealed the determination by the trial court, requesting an expedited review, but have elected not to request an injunction against the enforcement of the requirements of SB-1 pending completion of the appeal.

The decision by the trial court caught many financial intermediaries off guard—in no small measure because of the belief that SB-1 was clearly preempted by the FCRA. Accordingly, there is some level of concern regarding the appropriate degree of compliance that should be devoted to SB-1’s requirements pending the appeal and thereafter. This concern is based not only on the perspective that many companies’ privacy disclosures are less restrictive than the requirements of SB-1, but also from the realization that immediately complying with SB-1’s data transfer rules could limit the right of a company to transfer data in the future should the trial court’s determination be reversed.

While these and related tactical compliance questions certainly require attention, many institutions are struggling with the initial task of analyzing the privacy provisions of SB-1 in order to answer basic questions such as coverage and disclosure alternatives—including the task of parsing through SB-1’s perplexing and confusing organization.

This memorandum navigates through the substantive requirements of SB-1 and its general applicability to “financial institutions.” In addition, SB-1’s disclosure and timing requirements are analyzed in a manner intended to permit consideration of alternatives in order to achieve a reasonable degree of compliance.

Background

In September 2003, the California Legislature adopted SB-1, which by its terms expanded on the federal privacy protections adopted as Title V of the Gramm-Leach-Bliley Act (the “GLB Act”). (Substantially similar privacy protections were adopted by the federal banking agencies and other state and federal regulatory agencies responsible for implementation of the GLB Act’s privacy protections.)

Subsequent to the adoption of SB-1—but prior to its purported effective date of July 1, 2004—Congress adopted amendments to the Fair Credit Reporting Act (the “FCRA”), which amendments have become known as the “FACT Act.” One of the significant...
provisions of the FACT Act was an affiliate-sharing provision that arguably was intended to preempt state attempts to regulate affiliate-sharing with respect to the credit reporting process. Moreover, the intent of Congress that federal preemption should apply appeared to be clear because of language that indicated any topic specifically addressed in the FACT Act was preempted.

However, despite this strong legislative evidence, the trial court in Lockyer disagreed. Among other things, the court appeared to draw a distinction between privacy concerns that are not preempted by the GLB Act and the credit reporting functions that are addressed by the FCRA, as amended by the FACT Act. According to the court, because a data transfer between affiliated companies is not a credit report pursuant to the FCRA (i.e., data transfers among affiliates are excluded from the definition of a credit report), that exclusion of transferred data likewise excludes such data from any preemptive effect that either the FACT Act or the FCRA might have with regard to data transferred among affiliated companies for credit-related purposes.

The result—at least until an appeal is concluded—is now a bifurcated scheme whereby financial institutions conducting business in California must comply with the privacy requirements of SB-1—either by establishing California customer accounts as a subcategory for privacy purposes, or by extending SB-1’s privacy requirements to the institution’s entire database.

SB-1’s Requirements

SB-1 is more restrictive than the GLB Act and the FACT Act, and accordingly expands privacy protection for California consumers in two significant ways.

First, SB-1 provides that, prior to providing “nonpublic personal information” regarding a customer to an unaffiliated third party, a financial institution must receive an “opt-in” from a consumer; whereas, in the same circumstance, the GLB Act merely requires an “opt-out.” Second, with regard to sharing of nonpublic personal information with affiliated entities, SB-1 provides that a disclosure must first be provided to a consumer, and the consumer must be afforded a reasonable period of time to “opt-out” from affiliate-sharing. (It is important to note that each of these two requirements is subject to exceptions.)

Each of these requirements is discussed in greater detail below:

Sharing of Consumer Data with Unaffiliated Entities

Section 4052.5 of SB-1 establishes a general prohibition on the sharing of confidential consumer information with unaffiliated entities by stating:

Except as provided in Sections 4053, 4054.6, and 4056, a financial institution shall not sell, share, transfer, or otherwise disclose nonpublic personal information to or with any nonaffiliated third parties without the explicit prior consent of the consumer to whom the nonpublic personal information relates. (Emphasis added.)

If a financial institution wishes to share confidential consumer information with unaffiliated entities, and an exception to the general prohibition does not apply, the financial institution must provide the consumer with a disclosure permitting the consumer to affirmatively authorize the financial institution to share the information. This requirement—that a consumer must opt-in to information sharing—means that a financial institution cannot proceed with information sharing without first receiving the consent of its customer.

Sharing of Consumer Data with Affiliated Entities

In regard to sharing of consumer data with affiliated companies, Section 4053(b)(1) of SB-1 imposes an opt-out requirement:

A financial institution shall not disclose to, or share a consumer’s nonpublic personal information with, an affiliate unless the financial institution has clearly and conspicuously notified the consumer annually in writing.
pursuant to subdivision (d) 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 [w]eb site jointly operated or maintained under a common name by or on behalf of the financial institution and its affiliate, provided that where a consumer has exercised his or her right to prohibit disclosure pursuant to this division, nonpublic personal information is not further disclosed or used by an affiliate except as permitted by this division.7

Exceptions

It should be noted that there are several significant exceptions to the prohibitions on information sharing that may apply to financial institutions:

Operational and Account Processing Exceptions. A financial institution may share nonpublic personal information with affiliated and unaffiliated entities for usual and typical business purposes (similar to those purposes set forth in Title V of the GLB Act), provided that the following conditions are met:

- 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.8
- The nonpublic personal information is released with the consent of or at the direction of the consumer.9
- The nonpublic personal information is 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; and to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability.10
- 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 business or professional services, such as printing, mailing services, data processing or analysis, or customer surveys, on behalf of the financial institution, provided that several specific conditions are met.11

Joint Marketing Efforts. In regard to joint marketing efforts with unaffiliated entities, a partial exception is provided in that the requirement of a consumer to opt-in to sharing is converted into an opt-out so long as the consumer is provided the opportunity to opt-out. Pursuant to Section 4053(b)(2) of SB-1, a financial institution may jointly market with another unaffiliated financial institution as follows12:

- 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.
- The financial product or service is jointly offered, endorsed, or sponsored, and clearly and conspicuously identifies for the consumer the financial institutions that disclose and receive the disclosed nonpublic personal information.
- 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.

- The financial institution that releases the nonpublic personal information has complied with Section 4053(d) and the consumer has not directed that the nonpublic personal information not be disclosed.

- In spite of the foregoing, 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 Section 4053(b)(2) are met.13

Commonly Held and Operated Companies. Section 4053(c) of SB-1 sets forth a significant exception for commonly held companies engaged in the same line of financial services. That exception allows for the sharing of nonpublic personal information between commonly held and controlled companies within a holding company structure, provided that the following requirements are satisfied:

- The financial institution disclosing the nonpublic personal information and the financial institution receiving it are regulated by the same functional regulator.14

- The financial institution disclosing the nonpublic personal information and the financial institution receiving it are both principally engaged in the same line of business. For purposes of complying with SB-1, the "same line of business" must be one and only one of the following: (a) insurance; (b) banking; or (c) securities.15

- The financial institution disclosing the nonpublic personal information and the financial institution receiving it must share a common brand, excluding a brand consisting solely of a graphic element or symbol, within their trademark, service mark, or trade name, which is used to identify the source of the products and services provided. A wholly owned subsidiary shall include a subsidiary wholly owned directly or wholly owned indirectly in a chain of wholly owned subsidiaries.16

Marketing of Third Party Products and Services by a Financial Institution. Finally, Section 4053(e) of SB-1 permits a financial institution to market the products and services of both affiliated and nonaffiliated entities to its customers, provided that prudent safeguards are adopted to prevent the unauthorized use of consumer data for any purpose other than for the limited purpose of providing the product or service. Among other things, Section 4053(e) requires that the financial institution's marketing to its own customers have in place a contract with the third party that provides the financial institution the right to audit the unaffiliated company in order to verify compliance.17

California Disclosure Requirements—Substantive and Procedural

SB-1 provides that disclosures regarding the consumer's opt-out or opt-in rights must be provided to a consumer prior to the financial institution engaging in covered data transfer activities. In the case of an opt-out, the financial institution must provide the consumer with a disclosure form, and the financial institution must wait 45 days from the date the disclosure is sent prior to sharing nonpublic personal information.18

In the event the consumer's nonpublic personal information had been disclosed (because of the consumer not having chosen the opt-out election at a prior point in time) the consumer may, at any future time, choose the opt-out election. If the consumer so chooses to opt-out, the financial institution must comply with the consumer's request within 45 days of the financial institution's receipt of the consumer's request to not have his or her nonpublic personal information disclosed. (Because a consumer's opt-in right places the right to control data sharing exclusively with the consumer, there is no corresponding time period provided for in SB-1 with respect to the opt-in right of a consumer.)
It is important to note that—when attempting to comply with SB-1’s disclosure requirements, the statute includes a model form for the affiliated sharing disclosure, yet there is no standard form with respect to nonaffiliated sharing of nonpublic personal information. In the case of affiliated sharing, a financial institution choosing to draft its own disclosure may submit its draft form other than the statutory model form to its functional regulator and the receipt of approval creates a rebuttable presumption that the notice complies with the requirements of SB-1.19

Conflicting Laws: Practical Considerations Regarding Compliance

When considering compliance alternatives, the following observations are offered:

First, SB-1 is primarily a disclosure statute that imposes a mandatory notice to be provided to a consumer prior to sharing nonpublic personal information with affiliated or unaffiliated entities (and no exceptions otherwise apply). Therefore, a financial institution’s privacy policy must reflect SB-1’s substantive limitations, including the ability of a consumer to opt-out or to opt-in, in an appropriate manner. This presents the issue of whether to include a qualification regarding a California consumer’s privacy rights or to extend SB-1’s requirements to all consumers covered by the privacy disclosure. Moreover, in light of the appeal in the Lockyer case, care must be exercised so that if the Lockyer decision is reversed, a financial institution could return to a uniform approach regarding its privacy policies that would be applicable to all consumers.

Second, assuming that a financial institution determines that there are data-sharing activities that require providing a disclosure either in regard to affiliated data-sharing or unaffiliated data-sharing, SB-1 indicates that the appropriate disclosure must be provided prior to data-sharing taking place. In the case of affiliated data-sharing, where it is determined that an opt-out disclosure form must be sent to the consumer, a time period of 45 days is required between the delivery of an affiliated disclosure form and the initiation of data-sharing activities.20 In the case of unaffiliated data-sharing, no data-sharing is permitted unless and until an opt-in is received from each consumer.21

Third, as an additional degree of complexity, it should be noted that many commentators have pointed out that, while the bank trade group plaintiff's argument in the Lockyer case would negate the opt-out requirements for affiliate-sharing established by SB-1, there is no similar preemption argument available for the opt-in requirement applicable to data transfers to unaffiliated companies. Accordingly, even in the instance in which the trial court’s decision in Lockyer is reversed, financial institutions may still be required to differentiate between certain of their data-transfer policies applicable in California and those applicable elsewhere.

Fourth, SB-1 provides a safe harbor from liability22 in that a financial institution that does not engage in data-sharing activities requiring disclosures need not provide the disclosures until such time as the entity commences data sharing activities that require disclosure.23 Among other things, this means that a financial institution can manage its legal risk by prohibiting data-sharing that requires prior disclosure by prohibiting sharing until appropriate disclosures and time periods have been satisfied.

Finally, it is important to note that, when considering compliance initiatives, SB-1 is indicative of the interplay between privacy, data security and contract management. In order to comply with SB-1, not only must a financial institution adopt compliance procedures, but data security obligations regarding confidentiality and integrity are concomitant responsibilities. Moreover, SB-1 expands and refines concepts originally addressed in the GLB Act that will require that care be exercised when establishing contractual relationships with both affiliates and third parties to ensure that due diligence and verification obligations contained in SB-1 are enforceable.

* * * * * * *

Reed Smith, a leading global law firm with nearly 1,000 lawyers located in 15 U.S. and two U.K. cities, represents Fortune 100 as well as mid-market and emerging companies. Clients include technology companies and entrepreneurs, financial services firms, life sciences companies and health care providers and insurers,
communications companies, manufacturers, universities, non-profit organizations, real estate developers, and municipalities throughout the United States, the United Kingdom, and in 40 other countries. For more information, please visit reedsmith.com.

2  SB-1 modified the California Financial Code (the "Financial Code") by adding a new Division 1.2. For purposes of this memorandum, references to the provisions of SB-1 will refer to Division 1.2 of the Financial Code.
3  Under SB-1, nonpublic personal information is defined, among other things, as personally identifiable financial information: (a) provided by a consumer to a financial institution; (b) resulting from any transaction with the consumer or any service performed for the consumer; (c) 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: (i) federal, state, or local government records; (ii) widely distributed media; or (iii) disclosures to the general public that are required to be made by federal, state, or local law. Financial Code § 4052(a).
4  The term “financial institution” is broadly defined in the same manner as the term is defined by the GLB Act, and generally includes all entities that engage in banking, securities or insurance activities. Financial Code § 4052(c).
5  To the contrary, the FACT Act requires an “opt-out” for marketing by affiliates.
6  Financial Code § 4052.5.
7  Financial Code § 4053(b)(1).
8  Financial Code § 4056(b)(1).
9  Financial Code § 4056(b)(2).
10  Financial Code § 4056(b)(3).
11  Financial Code § 4056(b)(9).
12  Financial Code § 4053(b)(2).
13  It should also be noted that this exception only applies to joint marketing agreements with other financial institutions and not to joint marketing agreements with companies that operate outside of the banking, securities and insurance industries. Accordingly, if this exception is relied upon, care must be exercised to confirm that the activity is an approved activity for a bank, insurer, or securities firm.
14  With respect to the definition of the term “the same function regulator,” financial institutions regulated by the Office of the Comptroller of the Currency, Office of Thrift Supervision, National Credit Union Administration, or a state regulator of depository institutions shall be deemed to be regulated by the same functional regulator; financial institutions regulated by the Securities and Exchange Commission, the United States Department of Labor, or a state securities regulator shall be deemed to be regulated by the same functional regulator; and insurers admitted in California to transact insurance and licensed to write insurance policies shall be deemed to be in compliance with this provision of SB-1. Financial Code § 4053(c)(1).
15  Financial Code § 4053(c)(2).
16  Financial Code § 4053(c)(3).
17  Financial Code § 4053(e). This exception is, in effect, the converse of the joint marketing exception in that a financial institution is permitted to directly market products of third parties to its customers.
18  Financial Code § 4053(d)(2)(B). A financial institution using its own disclosure form must submit that document to the Office of Privacy Protection, which will post the disclosure on its website. It should be noted, however, that the availability of the rebuttable resumption of compliance has not been available to many covered financial institutions because of the refusal of many “financial regulators” to review and approve non-conforming disclosures.
19  Financial Code §§ 4053(b)(1), 4053(d). If annual written notice has not already been provided to the consumer, followed by a 45-day waiting period, a disclosure form must be sent to the consumer, followed by a 45-day waiting period, in order to comply with SB-1. Financial Code §§ 4053(b)(1), 4053(d).
A financial institution with assets in excess of $25,000,000 must include a self-addressed, first-class business reply return envelope with the notice. In lieu of the business reply return envelope, a financial institution may offer a self-addressed return envelope and at least two alternative cost-free means for consumers to communicate their privacy choice, such as calling a toll-free number, sending a fax to a toll-free number, or using electronic means such as a web site or e-mail address. A financial institution with assets of $25,000,000 or less must include a self-addressed return envelope with the notice. Financial Code § 4053(d)(6).

While beyond the scope of this memorandum, financial institutions should be aware that violations of SB-1 might also constitute violations of other provisions of California law that may address privacy, identity theft, and data security. These provisions include, but are not limited to, the broad unfair and deceptive business practice provisions set forth at California Business and Professions Code § 17200, as well as provisions of the California Constitution.

Please note the penalties set forth in SB-1 are outlined in Financial Code § 4057 as follows:

- A civil penalty not to exceed $2,500 for negligent disclosure of nonpublic personal information, in violation of SB-1, regardless of the amount of damages suffered by a consumer as a result of the violation. However, if the disclosure or sharing results in the release of nonpublic personal information of more than one individual, the penalty is not to exceed $500,000.

- A penalty of $2,500 per individual violation of SB-1, for knowingly and willfully obtaining, disclosing, sharing, or using nonpublic personal information, regardless for the amount of damages suffered by the consumer as a result of the violation.

- In determining the penalty to be assessed, the court may take into account the total assets and net worth of the violating entity; the nature and seriousness of the violation; the persistence of the violation (including any attempts to correct the situation leading to the violation); the length of time over which the violation occurred; the number of times the entity has violated SB-1; the harm caused to consumers by the violation; the level of proceeds derived from the violation; and the impact of the possible penalties on the overall fiscal solvency of the violating entity.

- In the case of identity theft, as defined by Section 530.5 of the California Penal Code, the foregoing penalties shall be doubled.

- A civil action to recover the penalties discussed above may be brought by the Attorney General or the functional regulator with jurisdiction over regulation of the financial institution as set forth in Financial Code § 4057(e)(2).