The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 16477

August 28, 2003

CALIFORNIA ENACTS PRIVACY LEGISLATION IMPOSING AN OPT IN ON SHARING WITH NONAFFILIATES AND AN OPT OUT FOR AFFILIATE SHARING

[16477] August 28, 2003 TO: COMPLIANCE ADVISORY COMMITTEE No. 67-03 OPERATIONS MEMBERS No. 25-03 PRIMARY CONTACTS - MEMBER COMPLEX No. 68-03 PRIVACY ISSUES WORKING GROUP No. 3-03 SEC RULES MEMBERS No. 113-03 SMALL FUNDS MEMBERS No. 43-03 TECHNOLOGY ADVISORY COMMITTEE No. 10-03 RE: CALIFORNIA ENACTS PRIVACY LEGISLATION IMPOSING AN OPT IN ON SHARING WITH NONAFFILIATES AND AN OPT OUT FOR AFFILIATE SHARING After four years of trying, California has enacted a privacy law that imposes on financial institutions privacy requirements that are more rigorous than those under federal law (i.e., the Gramm-Leach-Bliley Act ("GLB Act") and the regulations adopted thereunder) with respect to a financial institution's disclosure of nonpublic personal information about California residents.1 The effective date of this new law, the California Financial Information Privacy Act (the "Act"), which was signed by Governor Davis yesterday, is July 1, 2004. Generally speaking, the Act prohibits a financial institution from disclosing a California consumer's nonpublic personal information to: (1) a nonaffiliated third party unless the consumer has opted in to the sharing of such information; and (2) an affiliate unless the institution provides an annual notice as required by the Act to the consumer and offers the consumer the opportunity to opt out of the sharing.2 Several exceptions are provided to these general prohibitions. Importantly, the Act preempts all privacy ordinances enacted by local government entities in California, both retroactively and prospectively. The provisions of the Act are discussed in detail below. 1 A copy of the Act, which was enacted as California Senate Bill 1, can be found on the General Assembly's website at: http://www.assembly.ca.gov/acs/acsframeset2text.htm. As discussed in Section I of this memorandum (Definitions), the term "consumer" as used in the law only means consumers who reside in California. Passage of this law has resulted in the sponsors of a referendum on privacy that was to appear on California's March 2004 ballot agreeing not to pursue such referendum. (The signatures to place this issue on the ballot had been collected but, based upon passage of the Act, the referendum's sponsors agreed not to turn them into the California Secretary of State by the August 20th deadline for submitting such signatures.) This ballot initiative would have imposed an opt in requirement on sharing with nonaffiliates and an opt out provision on sharing with affiliates. 2 The Act expressly preserves the ability of financial institutions to market their own products and services or the products and services of others (affiliates and nonaffiliates) so long as no nonpublic information is disclosed in violation of the law. Also, as with privacy regulations under the GLB Act, the Act prohibits an entity that receives nonpublic information from another

financial institution from disclosing it to another entity unless such subsequent disclosure would be lawful if made directly by the financial institution to the other entity. 2 I. DEFINITIONS Section 4052 of the Act includes definitions for the following terms: “Nonpublic personal information” (NPI) “Personally identifiable financial information” “Financial institution” “Affiliate” “Nonaffiliated third party” “Consumer” “Control” “Necessary to effect, administer, or enforce”3 “Financial product or service” “Clear and conspicuous” and “Widely distributed media” These definitions are largely consistent with those in SEC Regulation S-P, which implements the privacy provisions of the GLB Act for investment companies, investment advisers and broker- dealers. One important difference, however, is that “consumer,” is defined to mean only those consumers who reside in California based upon their last known address, other than a military address. As such, the provisions of the Act only apply to the sharing and disclosure of NPI relating to persons residing in California. II. SHARING INFORMATION WITH NONAFFILIATED THIRD PARTIES – OPT IN REQUIRED A. General Prohibition Section 4052.5 of the Act prohibits a financial institution from selling, sharing, transferring, or otherwise disclosing NPI to or with any nonaffiliated third party “without the explicit prior consent of the consumer to which the [NPI] relates.” Exceptions to this general prohibition are discussed in subdivision C. of this section and in Section IV of this memorandum. Pursuant to Section 4053(a)(1) of the Act, a financial institution may not share a customer’s NPI unless it has first obtained a consent acknowledgment from the consumer that complies with the requirements of Section 4053(a)(2) of the Act, which is next discussed. 3 Consistent with the GLB Act’s definition of this term, the Act defines this term to mean (1) that 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 . . .; or (2) the disclosure is required or is a usual, appropriate, or acceptable method, in connection with 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. 3 B. Consent Acknowledgement Requirements Section 4053(a)(2) requires that, in order to disclose NPI to a nonaffiliated third party, a financial institution must utilize “a form, statement, or writing” that meets all of the following criteria: • It must be a separate document not attached to any other document; • It must be dated and signed by the consumer; • It must clearly and conspicuously disclose that, by signing, the consumer is consenting to the disclosure to nonaffiliated third parties of NPI pertaining to the consumer; • It must clearly and conspicuously disclose: (i) that the consent will remain in effect until revoked or modified by the consumer; (ii) that the consumer may revoke consent at any time; and (iii) the procedure for the consumer to revoke consent; and • It must clearly and conspicuously inform the consumer that (i) the financial institution will maintain the document, or a true and correct copy of it; (ii) the consumer is entitled to a copy of the document upon request; and (iii) the consumer may want to make a copy of the document for his or her own records. The Act prohibits a financial institution from discriminating against or denying a product or service to a consumer who does not opt in, unless the consumer’s consent is necessary to provide such product or service. The Act recognizes the ability of financial institutions to offer incentives or discounts in order to entice consumers to opt in to the sharing of their NPI. C. Exemption for Jointly Offered Products or Services In addition to the exceptions provided in Section 4056 of the Act, which permit the sharing of NPI regardless of whether it is with an affiliate or nonaffiliated third party, Section 4053(b)(2) provides an exemption from the Act’s prohibition on sharing or disclosing NPI to a nonaffiliated third party in order to jointly offer financial products or services. 4 In

particular, this provision permits the sharing of NPI without first obtaining the consumer's consent provided the sharing is pursuant to a written agreement between the parties involved in sharing the NPI and each of the following conditions is met:5 • The product or service offered is provided by at least one of the financial institutions that is a party to the written agreement; • The 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 NPI; 4 The conditions of this exemption largely track those in the "joint marketing" exemption of Regulation S-P (248.13), except that, unlike under Regulation S-P, the Act requires that consumers be provided the opportunity to opt out prior to the sharing of their NPI. The Act also includes specific provisions governing affinity programs in which there is an agreement between a financial institution and a business entity that is not a financial institution to offer a credit card in the name of the business entity. See Section 4054.6 of the Act. 5 Pursuant to Section 4053(b)(2)(E), these conditions do not apply to a financial institution that has a preexisting contract with a nonaffiliated third party to offer a product or financial service if the contract was entered into on or before January 1, 2004, so long as such sharing of the NPI occurs prior to January 1, 2005. Beginning on January 1, 2005, no NPI may be shared pursuant to such contract unless all the requirements listed in the text are satisfied. 4 • The written agreement provides that the financial institution receiving the NPI is required to maintain the confidentiality of the information and is prohibited from disclosing or using the NPI except to carry out the joint offering or servicing of a financial product or service that is the subject of the written agreement; and • The financial institution that releases the NPI has complied with the annual notice/opt out requirements imposed on financial institutions that share information with affiliates and the consumer has not opted out of such sharing. III. SHARING INFORMATION WITH AFFILIATES – ANNUAL NOTICE AND OPT OUT REQUIRED A. General Prohibition Section 4053(b)(1) of the Act prohibits a financial institution from disclosing to or sharing with an affiliate a consumer's NPI unless the financial institution "has clearly and conspicuously notified the consumer annually6 in writing . . . that the NPI may be disclosed to an affiliate of the financial institution and the consumer has not directed that the NPI not be disclosed." There are, however, exceptions to this general prohibition, which are discussed in subdivision F. of this section and in Section IV of this memorandum. To satisfy the annual notice requirement of Section 4053(b)(1), the financial institution must comply with the requirements set forth in Section 4053(d) of the Act, which are discussed below. A consumer may opt-out of the sharing of NPI at any time. A financial institution must provide a consumer a reasonable opportunity prior to disclosure of NPI to direct that his or her NPI not be disclosed, and a consumer's opt-out request must be honored within 45 days of its receipt. Such request shall be valid until amended by the consumer. A financial institution that does not have a continuing relationship with a consumer, other than the initial transaction in which the product or service is provided, is not required to provide an annual notice to the consumer as long as the financial institution provided the notice at the time of the initial transaction. As with the Act's opt in requirement, the Act prohibits a financial institution from discriminating against or denying a product or service to a consumer who has elected to opt out of the sharing of their information unless such sharing is necessary to provide the product or service. B. Required Contents of the Annual Notice Section 4053(d) governs the annual notice that a financial institution must provide prior to sharing or disclosing a consumer's NPI. A financial institution that uses the form set forth in the Act7 shall be "conclusively presumed" to have satisfied the Act's notice requirements. In 6 As used in the law, "annually" has the same meaning as in Regulation S-P – i.e., at least once in any period of 12 consecutive months. 7 When the bill was enacted by the General Assembly, this form was not included in it. Subsequent to the bill's passage, however, the sponsor held a press conference and distributed a form that, presumably, is the form

contemplated by the bill. A copy of this form is attached. 5 lieu of using the statutory form, a financial institution is required to use a one-page form satisfying each of the following requirements:8 • The form must use the title, “IMPORTANT PRIVACY CHOICES FOR CONSUMERS” and must use the following headers, if applicable: “Restrict Information Sharing With Companies We Own or Control (Affiliates);” and “Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products and Services;”9 • The titles and headers in the form must be clearly and conspicuously displayed and no text in the form may be smaller than 10-point type; • The form must be a separate document; • The choices provided in the form must be stated separately and may be selected by checking a box; • The form must be designed to call attention to the nature and significance of the information in the document; • The form must present information in clear and concise sentences, paragraphs, and sections; • The form must use short explanatory sentences (an average of 15-20 words) or bullet lists whenever possible; • The form must avoid multiple negatives, legal terminology, and highly technical terminology whenever possible; • The form must avoid explanations that are imprecise and readily subject to different interpretations; • The form (excluding the required title and headings) must achieve a minimum Flesch reading ease score of 50;10 and • The form must provide wide margins, ample line spacing, and use boldface or italics for key words. A financial institution’s notice must also clearly and conspicuously disclose the information necessary to direct the consumer on how to opt out, including any toll-free phone or fax number or website address, if those means of communication are offered by the financial institution. A financial institution may include in its form one or more brief examples or explanations of the purpose or purposes or context within which the information may be shared, as long as such examples satisfy the Act’s clarity and readability requirements. The Act permits the “householding” of notices, but its provisions do not appear entirely consistent with those under Regulation S-P. In particular, Section 4054(b) of the Act provides 8 As under Regulation S-P, a financial institution may provide a joint notice from it and one or more of its affiliates or other financial institutions identified in the notice so long as the notice is accurate with respect to the financial institution and the other entities referenced. 9 A financial institution that does not disclose or share NPI as described in a header may omit such header and the accompanying information box from the form. 10 The Flesch reading ease score rates text on a 100-point scale; the higher the score, the easier it is to understand the document, with 60 to 70 generally being considered an acceptable score for literate adults. The formula for computing the Flesch reading ease score is: 206.835 – (1.015 x ASL) – (84.6 x ASW) where ASL is the average sentence length (the number of words divided by the number of sentences) and ASW is the average number of syllables per word (the number of syllables divided by the number of words). 6 that a notice provided to a member of a household shall be considered a notice to all members of the household unless the household contains “another individual who also has a separate account with the financial institution.”11 C. Filing Requirement A financial institution using a form other than the statutory form: (1) must file it with the California Office of Privacy Protection12 within 30 days after it is first used; and (2) may submit it to the financial institution’s functional regulator13 for approval. D. Requirements Imposed on the Envelope Containing the Annual Notice14 The Act also regulates the envelope in which the annual notice is sent to the consumer. In particular, Section 4053(d)(2)(D) provides that the outside of such envelope must clearly state in 16-point boldface type “IMPORTANT PRIVACY CHOICES,” unless the notice is sent in the same envelope as a bill, account statement, or application requested by the consumer, in which case this wording may be omitted. The notice shall be sent in any of the following ways: • With a bill, other statement of account, or application requested by the consumer, in which case the privacy notice required by the GLB Act may be included in the same envelope; • As a separate notice or with the GLB Act privacy

notice, so long as only information related to privacy is included in the envelope; or • With any other mailing, in which case it shall be the first page of the mailing. E. Required Response Options The Act mandates the response options that a financial institution must provide to a consumer receiving the annual notice who elects to opt out of the sharing of NPI. These requirements vary depending upon the financial institution's assets. In particular, if the financial institution's assets are more than $25 million, it must either (1) include a self-addressed first class business reply return envelope (i.e., a postage-paid envelope) with the notice or (2) include a self-addressed envelope (but not postage-paid) with the notice and provide at least two alternative cost-free means by which customers may opt out – e.g., a toll-free phone 11 By contrast, Regulation S-P permits householding if: (1) the privacy notice is in or accompanies a shareholder report or a prospectus delivered under the SEC's householding rules; or (2) the fund, consistent with the SEC's householding rules, had obtained consent from the household to household other documents. See Regulation S-P at 248.9(c) and Question 7 of "SEC Staff Responses to Questions About Regulation S-P," which may be found on the SEC's website at: http://www.sec.gov/divisions/investment/guidance/regs2qa.htm. 12 The California Office of Privacy Protection is a state agency created in 2000 to promote and protect the privacy rights of consumers. Its address is: Office of Privacy Protection, Department of Consumer Affairs, 400 R Street, Suite 3080, Sacramento, CA 95814. Additional information about this agency can be found on its website: http://www.privacy.ca.gov/. 13 While Section 4053(c) defines "functional regulator" for the securities industry to mean the SEC and the California Corporation Commission, presumably this reference to the institution's "functional regulator" means the California Corporation Commission. 14 The law expressly permits the electronic delivery of notices provided certain conditions are met, including compliance with the Federal Electronic Signatures in Global and National Commerce Act. See Section 4054 (c) for additional conditions. 7 number, a fax number, or an electronic response. A financial institution with assets of up to and including $25 million is only required to provide a self-addressed envelope with the notice. F. "Silo" Exemption Section 4053(c) of the Act provides an exemption, referred to as a "silo" exemption, from the Act's prohibitions for the sharing or disclosing of NPI to a related entity that is subject to the same functional regulator as the entity disclosing the information and that is in the same line of business as the sharing entity. In particular, Section 4053(c) provides that the prohibitions of Section 4053 shall not "restrict or prohibit the sharing of [NPI] between a financial institution and its wholly owned financial institution subsidiaries; among financial institutions that are each wholly owned by the same financial institution; among financial institutions that are wholly owned by the same holding company; or among the insurance and management entities of a single insurance holding company system . . ."15 provided that, in each case, the financial institution disclosing the NPI and the institution receiving it: • Are regulated by the same functional regulator;16 • Are both principally engaged in the same line of business – i.e., one and only one of the following: insurance, banking, or securities; and • 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. IV. EXCEPTIONS In addition to the silo exemption available to related entities and the exemption for sharing with nonaffiliated entities for purposes of jointly offering a product or service discussed above, the Act contains several exceptions, which are found in Section 4056 of the bill. Importantly, persons that qualify for an exception are relieved from all of the Act's obligations relating to notice, consent (opt in), and opt out. These exceptions largely track those available under the GLB Act and permit a financial institution to release NPI under various circumstances including: • Its release 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 (see Paragraph (b)(1)); • The NPI 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 (see Paragraph (b)(3)(A)); • The NPI is released to protect against actual or prevent actual or potential fraud, identity theft, unauthorized transactions, claims or liability or is released for required 15 Note that this provision does not use the term "affiliate" to describe the various relationships that may rely upon this exemption. Also, as used in this provision, a "wholly owned subsidiary" includes a subsidiary wholly owned directly or wholly owned indirectly in a chain of wholly owned subsidiaries. 16 According to this provision "financial institutions regulated by the SEC, the United States Department of Labor, or a state securities regulator are deemed to be regulated by the same functional regulator." 8 institutional risk control or for resolving customer disputes or inquiries (see Paragraphs (b)(3)(B) and (C)); • The NPI is released to persons holding a legal or beneficial interest relating to the consumer or to a person acting in a fiduciary or representative capacity on behalf of the beneficiary (see Paragraphs (b)(3)(D) and (E)); • The NPI is released to the extent permitted or required by Act, including to functional regulators and self-regulatory organizations (see Paragraphs (b)(5) and (7)); • The NPI 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 NPI concerns solely consumers of the business or unit (see Paragraph (b)(6)); • The NPI is released to an affiliate or nonaffiliated third party in order for the affiliate or the 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 all of the following requirements are met: (1) The services to be performed by the affiliate or nonaffiliated third party could lawfully be performed by the financial institution; (2) 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 NPI other than to carry out the purpose for which the financial institution disclosed the information, as set forth in the written contract; (3) The NPI provided to the affiliated or nonaffiliated third party is limited to that which is necessary for such entity to perform the services contracted for on behalf of the financial institution; and (4) 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 NPI. (See Paragraph (b)(9)); • The NPI is released as required by the USA PATRIOT Act (see Paragraph (b)(12)); or • The NPI is released in connection with a written agreement between a consumer and a federally registered broker-dealer or investment adviser to provide investment management services, portfolio advisory services, or financial planning and the NPI is released for the sole purpose of providing the products and services covered by the agreement (see Paragraph (b)(14)). V. LIABILITY/SANCTIONS Section 4057 of the Act governs the consequences for disclosing or sharing information in violation of the Act and permits the imposition of civil monetary penalties, which may be exclusively assessed and recovered in a civil court action brought by either the California Attorney General or the financial institution's functional regulator. (For the securities industry, this is the California Department of Corporations.) As such, there is no private right of action under the Act. The monetary penalties that may be assessed, irrespective of the amount of damages suffered by a consumer, are: 9 • For negligent disclosure or sharing – an amount not to exceed $2500 per violation or a total of $500,000; • For willfully disclosing, sharing, obtaining or using17 NPI in violation of the Act – an amount not to exceed $2500 per violation, with no cap on the maximum penalty. In the event the disclosure results in the theft of a consumer's identity, the above penalties shall be doubled. The Act also lists various factors a court must take into account in

assessing penalties. These factors include: the total assets and net worth of the violating entity; the nature, seriousness, length, and persistence of the violation; corrective action taken; the harm caused to consumers; and “the impact of penalties on the overall fiscal solvency of the violating entity.” VI. LOCAL ORDINANCE PREEMPTION Section 4058.5 of the Act preempts – both prospectively and retroactively – all local agency ordinances and regulations relating to the use and sharing of NPI by financial institutions. Accordingly, privacy ordinances enacted by the various local government entities in the San Francisco Bay area over the past two years are wholly preempted by this Act. VII. SEVERABILITY/FEDERAL PREEMPTION Section 4059 of the Act provides that the Act’s provisions are severable and, if any portion of the Act is deemed to be invalid or preempted by federal law, such invalidity shall not affect the remainder of the Act. This provision is significant in light of the recent ruling of the U.S. District Court for the Northern District of California, which held that local governments in California are preempted under the Fair Credit Reporting Act (FCRA) from restricting the sharing of information between financial institutions and their affiliates.18 Based upon the preemptive language in the FCRA, this holding may extend beyond the local ordinances that were at issue in the case to state laws such as California’s new Act, that restrict the sharing of information among affiliates. If so, this would mean that the provisions in this Act governing the sharing of information between financial institutions and their affiliates may violate the FCRA. Tamara K. Salmon Senior Associate Counsel Note: Not all recipients receive the attachment. To obtain a copy of the attachment, please visit our members website (http://members.ici.org) and search for memo 16477, or call the ICI Library at (202) 326-8304 and request the attachment for memo 16477. Attachment (in .pdf format) 17 Note, however, that nothing in the law prohibits any person from “obtaining” or “using” NPI. 18 See Bank of America et al. v. City of Daly City, California, et al. Nos. C 02-4343 CW; C 02-4943 CW (ND CA July 29, 2003). See also Institute Memorandum No. 16383, dated July 30, 2003, for a summary of this case and a copy of the court’s decision.
