

SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

SB 793 (Glazer)
Version: April 17, 2023
Hearing Date: April 25, 2023
Fiscal: Yes
Urgency: No
CK

SUBJECT

Insurance: privacy notices and personal information

DIGEST

This bill codifies an existing regulation requiring insurers to provide annual privacy notices to customers. However, it eliminates this requirement for insurers meeting certain conditions.

EXECUTIVE SUMMARY

The Insurance Information and Privacy Protection Act (IIPPA) establishes standards for the collection, use and disclosure of information gathered in connection with insurance transactions and seeks to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices. To this end, the IIPPA requires certain consumer protections be afforded in connection with information exchanged between insurance companies and their policyholders.

Insurers are required to provide timely notices regarding information practices and annual privacy notices to consumers. IIPPA regulations lay out the guidelines for when these notices are required and what is required to be included in them. At the federal level, the Graham-Leech Bliley Act (GLBA) also requires insurers to send specified privacy notices at certain points.

This bill seeks to codify a change to the GLBA that loosens the regulatory requirement that insurers provide annual notices to customers. The bill also narrows what is required to be provided under the joint privacy notices pursuant to the IIPPA.

This bill is author-sponsored. It is supported by various insurance company associations, including the Personal Insurance Federation of California. There is no known opposition. This bill passed out of the Senate Insurance Committee on a 7 to 0 vote.

PROPOSED CHANGES TO THE LAW

Existing law:

- 1) Establishes the Insurance Information and Privacy Protection Act (IIPPA), to establish standards for the collection, use, and disclosure of information gathered in connection with insurance transactions and to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices. (Ins. Code § 791.)
- 2) Requires an insurance institution or agent to provide a notice of information practices to all applicants or policyholders in connection with insurance transactions at the time of delivery or initial data collection and at the point of renewal, reinstatement, and change in benefits, as provided. (Ins. Code § 791.04.)
- 3) Authorizes an insurer to disclose personal or privileged information about an individual, which is collected or received in connection with an insurance transaction, as provided. This includes the authority to share personal or privileged information about an individual with an unaffiliated third party whose only use of the information will be in connection with the marketing of a product or service, as long as the individual is given an opportunity to opt out of this information-sharing. (Ins. Code § 791.13.)
- 4) Requires, pursuant to IIPPA regulations, that insurers provide a notice that accurately reflects its privacy policies and practices at the initiation of the customer relationship, annually thereafter, and when certain revisions are necessary. (10 C.C.R. §§ 2689.5, 2689.6, 2689.9.) The notices must include certain minimum information. (10 C.C.R. § 2689.7.)

This bill:

- 1) Codifies the annual notice requirement laid out in 10 C.C.R. § 2689.6.
- 2) Provides that an insurance institution or agent shall be deemed to comply with this requirement if all of the following conditions are met:
 - a) the insurance institution or agent does not provide medical-record, personal, or privileged information to a nonaffiliated third party pursuant to Section 791.13(k);
 - b) the insurance institution or agent additionally provides, as part of any abbreviated notice provided pursuant to Section 791.04, the internet website address to the insurance institution's or agent's complete privacy notice that complies with the underlying regulation and informs the consumer of each of the following rights in a clear and conspicuous manner:

- i. the right to submit a written request to access, correct, amend, or delete the consumer's personal information and the manner in which the right may be exercised, including the contact information and the mailing address, internet website address, or both, where the consumer may submit a request;
 - ii. the right to receive a response within 30 business days of the consumer submitting a request to access, correct, amend, or delete their personal information;
 - iii. if the insurance institution refuses the consumer's request, the right to file a statement regarding what the consumer believes to be accurate and fair information and why the consumer disagrees with the insurance institution's refusal.
 - c) the insurance institution's or agent's policies and practices about disclosing personal or privileged information have not changed from the previous notice provided.
- 3) Provides that an insurance institution is not required to provide the notice to a former customer with whom it no longer has a continuing relationship.

COMMENTS

1. Privacy notices under the IIPPA and its regulations

The IIPPA was established with several central purposes:

- to establish standards for the collection, use, and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance-support organizations;
- to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize intrusiveness;
- to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy;
- to limit the disclosure of information collected in connection with insurance transactions; and
- to enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision.

The IIPPA and its attendant regulations carefully outline requirements for insurance companies and agents to provide consumers privacy notices at various points during the customer relationship.

One regulation requires an initial privacy notice. A licensee must “provide a clear and conspicuous notice that accurately reflects its privacy policies and practices” to a customer at the point when a customer relationship is established, except as provided.¹ This must happen before any nonpublic personal information is disclosed to a nonaffiliated third party.

Beyond that initial contact point, regulations require insurers to provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship.² The regulations also provide for revised notices when certain disclosures of personal information about a consumer are planned.³

The regulations dictate the minimum information that needs to go into these initial, annual, and revised notices. Some of the required components are:

- the categories of nonpublic personal information that the licensee collects;
- the categories of nonpublic personal information that the licensee discloses;
- the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information, and the general types of businesses in which the third parties engage, as provided;
- if a licensee wishes to disclose or reserve the right to disclose nonpublic personal financial information to an affiliate for marketing purposes without affirmative authorization or the right to opt out of that disclosure, a statement explaining that the licensee may disclose nonpublic personal financial information to affiliates for marketing purposes without obtaining prior authorization and the law does not allow customers to restrict that disclosure;
- an explanation of the consumer's right to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;
- the licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information, including a general description as to who is authorized to have access to the information; and
- if applicable, a statement that the consumer has the right to access and request correction of recorded nonpublic personal information and a brief description of the manner in which those rights may be exercised.⁴

These notice regulations all make clear that they are in addition to any notices required by Section 791.04 of the Insurance Code. However, they provide for both notices to be provided in a single combined notice meeting both sets of requirements. Section 791.04

¹ 10 C.C.R. § 2689.5.

² 10 C.C.R. § 2689.6.

³ 10 C.C.R. § 2689.9.

⁴ 10 C.C.R. § 2689.7.

requires an insurance institution or agent to provide a notice of information practices to all applicants or policyholders in connection with insurance transactions. This must happen at the time of delivery of the policy or certificate when personal information is collected from the applicant, an insured, or from public records. Otherwise, it must be provided at the point of collection from other sources.

Section 791.04 also requires provision of the notice of information practices upon renewal, reinstatement, or a change in benefits unless personal information is only collected from the policyholder, insured, or public records, or notice has already been given in the preceding 24 months.

The Section 791.04 notice must be in writing and state specified information, including whether personal information may be collected from persons other than the individual, the types of personal information that may be collected and disclosed, and a description of the individual's rights. However, in lieu of this detailed notice, insurers are authorized to provide an abbreviated notice informing the applicant or policyholder that personal information may be collected from other sources and disclosed without authorization, and that the applicant or policyholder has the right to access and correct all personal information collected and to request a detailed notice of information practices.

2. Codifying and carving out IIPPA regulations

This bill codifies the GLBA regulation regarding annual notices to customers. However, subdivision (c) in the bill exempts insurance institutions and agents from the requirement if the following conditions are met:

- the insurance institution or agent does not provide medical-record, personal, or privileged information to a nonaffiliated third party;
- the insurance institution or agent additionally provides, as part of the abbreviated notice (discussed above), the internet website address to the insurance institution's or agent's complete privacy notice that complies with the underlying regulation and informs the consumer of specified rights in a clear and conspicuous manner; and
- the insurance institution's or agent's policies and practices about disclosing personal or privileged information have not changed from the previous annual notice.

The description of rights is not a full and complete description of the rights that consumers have under the IIPPA. The abbreviated notice must notify consumers that they have the right to submit a written request to access, correct, amend, or delete the consumer's personal information and the manner in which the right may be exercised. This must include the contact information and the mailing address, internet website address, or both, where the consumer may submit a request. Consumers must also be

notified that they have the right to receive a response within 30 business days of the consumer submitting a request to access, correct, amend, or delete their personal information, and if the insurance institution refuses the consumer's request, the right to file a statement regarding what the consumer believes to be accurate and fair information in support of their request and why the consumer disagrees with the insurance institution's refusal.

According to the author:

Notices to consumers are only effective so long as they are meaningful. A phenomenon has been noted that the more frequent, numerous, lengthy notices are the less likely consumers are to read them. Given the importance of privacy notices, it is critical that notice for privacy rights be enacted and distributed in a manner most likely to inform consumers. In 2015 the federal government adopted an amendment to the Graham-Leach-Bliley Act (GLBA), the federal privacy protection act that insurers are beholden to, which would allow insurers to send their annual GLBA notices only when there is a change to the privacy policy. The intent is to flag to consumers that there is a change and that the notice requires their attention. California is one of three states that has not adopted the amendment to the GLBA, frequently referred to as the FAST Act amendment. SB 793 would remedy this and integrate the amendment into California law, and also require that an abbreviated privacy notice be sent to consumers to ensure there is continuous notice of how to access the full description of rights.

This change in the law is based loosely on changes made to the GLBA at the federal level, which eliminated the requirement for insurers to send annual GLBA privacy notices in most instances. AB 2372 (Calderon, 2022) was nearly identical to the existing bill. However, it required a more holistic description of a consumer's legal rights with regard to their information. The bill was not taken up for a vote on the Senate Floor and died on the Inactive File.

Writing in support, a coalition of insurance company associations, including the American Property Casualty Insurance Association, asserts:

California's requirements for consumer privacy notices were prompted, in part, by the federal Gramm-Leach-Bliley Act (GLBA), which was enacted in 1999. That statute sets forth certain privacy requirements for financial institutions, but with respect to insurers, enforcement was left to state insurance regulators. As originally enacted, GLBA required financial institutions to provide consumers with copies of their privacy policies annually. However, over time, both financial institutions and many consumer representatives came to recognize that the provision of annual

privacy notices was counterproductive as consumers received so many notices so frequently that they tended to disregard them. As a result, Congress amended GLBA in the Fixing America's Surface Transportation (FAST) Act in 2015. As amended, GLBA now requires financial institutions to provide consumers with one notice initially and additional notices thereafter only when there is a change in the privacy policies (provided the insurer shares nonpublic personal information with nonaffiliated third parties only in accordance with existing state regulations and statutes). Otherwise, the federal requirement for annual notices was repealed.

After passage of the federal FAST Act, the National Association of Insurance Commissioners (NAIC) followed with corresponding amendments to its model bulletin recommending that states adopt the revised privacy notice requirements.

SB 793 will bring California insurance law into line with GLBA, and changes made in many other states' insurance privacy laws by requiring insurers to send privacy policy notices once initially and thereafter only when a change has been made in the policy.

It should be noted that while the bill takes away an existing consumer protection, an important condition of the exemption is that the insurer must include, in any abbreviated notice they provide, a description of the consumer's core rights to access and correct information including the manner in which those rights can be exercised.

SUPPORT

ACLHIC
American Council of Life Insurers
American Property Casualty Insurance Association
Pacific Association of Domestic Insurance Companies
Personal Insurance Federation of California

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

AB 2372 (Calderon, 2022) *See* Comment 2.

AB 1184 (Chiu, Ch. 190, Stats. 2021) enhanced protections relating to health care service plans and health insurers accommodating requests from subscribers, enrollees, and insureds for the confidential communication of certain medical information. The bill required health plans/insurers to direct all communications regarding a protected individual's receipt of sensitive health care services directly to the protected individual, and prohibited the disclosure of that information to the policyholder without the authorization of the protected individual.

PRIOR VOTES:

Senate Insurance Committee (Ayes 7, Noes 0)
