

## Bulletin 308

### Consumer Privacy Obligations of Regulated Insurance Entities

This Bulletin is being issued to clarify the privacy obligations of regulated insurance entities under state and federal law with respect to insurance consumers. In addition to the existing Maine Insurance Information and Privacy Protection Act, 24-A M.R.S.A. §§ 2201–2220 (the "Maine Insurance Privacy Act"), two recent privacy initiatives provide new consumer protections in all sectors of the financial services market, including insurance. At the federal level, Title V of the federal Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, was enacted in 1999, and compliance became mandatory as of July 1, 2001. At the state level, "An Act to Conform the State's Financial Services Privacy Laws with Federal Law," P.L. 2001, c. 262 (L.D. 1640), was signed into law by Governor Angus S. King, Jr. on May 24, and takes effect on September 21, 2001 (the "Maine Financial Services Privacy Act").

(1) How does the new Maine Financial Services Privacy Act affect insurance? The effect of Chapter 262 on insurance is less extensive than on other financial services sectors, because the Maine Insurance Privacy Act has been in place for the life and health insurance industry. The principal insurance-related provision of the Maine Financial Services Privacy Act extends the scope of the Maine Insurance Privacy Act to include property and casualty insurance. Since the Maine Insurance Privacy Act is based on an NAIC Model Act used in a number of states, many property-casualty companies have already structured their operations so as to be in substantial compliance. Little or no change may be necessary for those companies after Chapter 262 takes effect. In addition, the Maine Financial Services Privacy Act clarifies the Superintendent's rulemaking authority to implement the provisions of the Gramm-Leach-Bliley Act. The Superintendent is currently evaluating the need for rulemaking, and expects to announce a proposal later this summer.

(2) Who is a covered insurance consumer? The Maine Insurance Privacy Act and the Gramm-Leach-Bliley Act apply only to insurance consumers: individuals who have been involved in insurance transactions for personal, family, or household purposes. This includes, but is not limited to, individuals who have shopped for or purchased personal lines coverage (even if the policy also provides incidental coverage for certain business activities), who are certificateholders under group life and health policies, or who have filed personal injury or workers' compensation claims against insurance policies or state-regulated self-insurance plans. However, individuals covered by self-funded private employer health plans are not considered insurance consumers, because federal law (ERISA) exempts those plans from state regulation. Finally, although the consumer privacy laws do not cover commercial policyholders or liability claims filed by business entities, carriers and insurance professionals should be aware that if they have collected health information on individuals who are not consumers, such information remains protected under Maine law, 22 M.R.S.A. § 1711-C.

(3) When and how may personal information be shared? The Gramm-Leach-Bliley Act provides that "It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." The privacy laws establish four basic categories of disclosures of personal information. In all cases, the disclosure must be made in a manner that protects the confidentiality of the information and, in the words of the Maine Insurance Privacy Act, must be "made with due consideration for the safety and reputation of all persons who may be affected by the disclosure [and] limited to the minimum amount of personal information necessary to accomplish a lawful purpose." 24-A M.R.S.A. § 2215(1).

- Disclosures "permitted by law" – a variety of disclosures made for limited purposes in the ordinary course of business, such as underwriting, claims handling, information processing, and fraud prevention. These may be described in generic terms in the regulated insurance entity's notice of information practices.
- Disclosures to affiliates for marketing purposes – such disclosures may not include health information. Consent is not required under state law or the Gramm-Leach-Bliley Act as long as the privacy notice provides an adequate explanation. Similar standards apply if you disclose personal information to nonaffiliated "service providers" for purposes of marketing your own

products and services.

- "Opt-out" – information may be disclosed for marketing purposes to non-affiliated third parties on an "opt-out" basis, as discussed more fully below, but only if it does not include health information or information about character, personal habits, mode of living, or general reputation. Under the Maine Insurance Privacy Act, the consumer has the right to opt out even if the third party has entered into a joint marketing agreement.
- "Opt-in" – anything that does not fall into the other three categories requires the affirmative written consent of the consumer; the law provides minimum standards for release forms. In situations where there may be a conflict of interest, consent must be given personally and not by a family member. When there is a legitimate business purpose – for example, access to health history when underwriting a life insurance application – the law does not prohibit a company from requiring the consumer to "opt in" to certain information disclosures as a condition of doing business.

(4) What should have happened by July 1, 2001? The Gramm-Leach-Bliley Act gives consumers two basic rights: the right to receive notices of information practices, and the right to withhold consent to certain disclosures of nonpublic personal information. Regulated insurance entities that are currently subject to the Maine Insurance Privacy Act, or which voluntarily adhere to nationwide standards consistent with the NAIC Model Privacy Act, should already be in substantial compliance with most Gramm-Leach-Bliley requirements. The most significant new federal requirement is that the reminder notices to existing customers, which under state law may be provided every other renewal cycle, must now be given at least annually. Although compliance with the Maine Insurance Privacy Act is voluntary for the property-casualty industry until September 21, compliance with Gramm-Leach-Bliley is now mandatory for all lines of insurance. Therefore, if regulated insurance entities were sharing any personal information that has become subject to a consent requirement, they must have ceased doing so by July 1, 2001 unless the individual has already been given notice and a reasonable opportunity to opt out (in cases where an opt-out standard applies) or the individual has given affirmative written or recorded electronic consent.

(5) How does the opt-out process work? If a regulated insurance entity, as defined by 24-A M.R.S.A. § 2204(23) ("licensee"), wishes to share nonpublic personal information about insurance consumers with nonaffiliated third parties for marketing purposes (including the sale of customer lists), each consumer who is affected, including former customers, must first be given the right to "opt out" of such disclosures. Certain information sharing with affiliates may also be subject to an opt-out requirement under the federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. In addition, some companies for business reasons may voluntarily provide an opportunity to opt out of some information sharing with affiliates. In order for the consumer's implied consent to be valid, there must be a clear and conspicuous notice describing what information the licensee wishes to share for what purposes, and how the consumer may exercise his or her right to opt out. The licensee must provide a reasonable means to opt out, such as a clearly labeled toll-free number or a simple response form, and wait a reasonable period of time (30 days is considered sufficient) before sharing information if the consumer does not respond. Consumers may not be discriminated against if they choose to opt out. Under the Maine Insurance Privacy Act, even if the consumer has declined to opt out, information shared by implied consent may not include health information or information about character, personal habits, mode of living, or general reputation.

(6) Must carriers and producers both provide notice to the same consumers? It depends on the producer's information practices. Insurance producers or agencies do not have to provide a separate set of notices as long as the carriers they represent give adequate notice and the producers do not use or disclose a consumer's personal information in a manner inconsistent with the notice(s) the consumer receives from the carrier(s). However, if the producer is also going to disclose personal information for its own purposes – for example, if the producer sells customer lists to third parties – then the producer will have to provide notice, and when information is being shared for marketing purposes with nonaffiliated third parties, the producer must also provide an opportunity for consumers to opt out.

(7) Who is entitled to receive privacy notices? Any consumer who is a "customer" (a policyholder or someone else with an ongoing business relationship) is entitled to receive a copy of the regulated

insurance entity's notice of information practices and privacy rights at the time the customer relationship is formed and annually thereafter. In addition, other consumers (including but not limited to applicants who do not purchase coverage, certificateholders under employee group policies, and third-party or workers' compensation claimants) are entitled to receive a copy of the notice if the regulated insurance entity either: (1) wishes to share personal information beyond the "disclosures permitted by law" in the necessary course of business; (2) collects additional information from sources other than the consumer; or (3) has selected the consumer for solicitation using criteria based on nonpublic personal information. Notice should also be provided to group policyholders and employee benefit plan sponsors. For individuals who are not customers or whose customer relationship has ended, a brief summary may be provided in situations where providing the complete privacy notice is unduly burdensome, if the consumer is notified that the complete notice is available upon request.

(8) What needs to be in the notice? In order to comply with both the Gramm-Leach-Bliley Act and the Maine Insurance Privacy Act, a notice of information practices and privacy rights should contain, at a minimum, the following information:

- A statement of the licensee's policies and practices with respect to disclosing nonpublic personal information to affiliates and nonaffiliated third parties, encompassing the specific information set forth below;
- The categories of information that may be disclosed;
- The categories of persons to whom the information may be disclosed, other than "disclosures permitted by law" in the necessary course of business;
- A summary of any disclosures "permitted by law" which are made with such frequency as to constitute a general business practice;
- A description of any disclosures of personal information made for marketing purposes, and any applicable opportunity to opt out;
- The licensee's policies and practices with regard to information on former customers;
- The categories of nonpublic personal information that are collected;
- Whether such information may be collected from sources other than the consumer, and if so, how;
- A statement explaining the consumer's right to access and request correction of recorded personal information;
- If applicable, a statement that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons;
- The policies the licensee maintains to protect the confidentiality and security of nonpublic personal information; and
- The disclosures required, if any, under the federal Fair Credit Reporting Act

While not required, a contact number and/or website link for additional information is highly encouraged.

(9) Can multistate privacy notice forms be used in Maine? Because the Maine Insurance Privacy Act exceeds the minimum requirements of Gramm-Leach-Bliley, standard multistate Gramm-Leach-Bliley notice forms will generally not be fully compliant with state law. Rather than prepare an entirely different form, licensees may use the multistate form along with a state-specific supplement, as long as the notice taken as a whole is clear and understandable to the consumer. If there is any conflict between the multistate form and the Maine supplement, the consumer must be given clear and conspicuous notice that the Maine supplement controls, and inconsistent provisions in the multistate form do not apply in Maine.

(10) What additional rights are provided under the Maine Insurance Privacy Act? In addition to providing notice rights and confidentiality rights related to those provided by the Gramm-Leach-Bliley Act, regulated insurance entities should be aware that in Maine, as in other states that have enacted

insurance privacy laws based on the NAIC Model Privacy Act, consumers have the following additional rights:

- The right to obtain access to recorded personal information in the possession or control of a regulated insurance entity, to request correction if the consumer believes the information to be inaccurate, and to add a rebuttal statement to the file if there is a dispute;
- The right to know the reasons for an adverse underwriting decision. Previous adverse underwriting decisions may not be used as the basis for subsequent underwriting decisions unless the carrier makes an independent evaluation of the underlying facts; and
- The right, with very narrow exceptions, not to be subjected to pretext interviews.

(11) Please remember the consumer perspective! Both in Maine and in other states, consumers have found some of the notices they have received to be quite confusing. Concerns raised include print that is too small, inadequate explanations of opt-out rights, and notices that are easily overlooked because they are surrounded by other promotional material. It is essential for insurers and insurance professionals to review their practices and procedures to make sure that consumers receive privacy notices that are clear and easily understood, and to remember that even the best written material is not always sufficient; there must be well-trained staff who are ready and able to respond to consumer inquiries.

July 12, 2001 \_\_\_\_\_  
ALESSANDRO A. IUPPA  
Superintendent of Insurance

NOTE: This bulletin is intended solely for informational purposes. It is not intended to set forth legal rights, duties, or privileges, nor is it intended to provide legal advice. Readers are encouraged to consult applicable statutes and rules and to contact the Bureau of Insurance at (207) 624-8475 if they need additional information.