CARLTON FIELDS

NAIC's New Cybersecurity Model Law Draft Is Still Flawed

September 02, 2016

Insurers are a prime target for hackers as a result of the vast stores of valuable data they maintain. Not all information is created equal, and it varies in value. Hacker services and software, illegal drugs, cyberweapons and all kinds of other types of stolen, confidential and compromised information is monetized and traded daily on darknet markets using various forms of cryptocurrency, by governments, hackers, criminals and businesses. While a stolen credit card number has value (which diminishes over time), it has much lower value than, for example, a personal medical file that might contain your "fullz" (date of birth, social security number, bank account information), which is less mutable, and therefore maintains its value. But insurers often possess much more than your "fullz." Life insurers, for example, possess everything from medical files for underwriting to financial account information for payment processing. They may even possess real-time information about a consumer's physical state of being, from heart rate to "steps," tracked through a Fitbit or similar device. Property casualty insurers may possess everything from real-time telematics of how and where a consumer is driving, to floor plans and physical security blueprints of businesses and their policy limits for kidnap/ransom insurance, or a consumer's place of work, work hours, home security system information and more. This type of information has as much value as the value of exploiting it will allow. Unsurprisingly, insurer data breaches are frequently in the news. Anthem Inc. is by no means the only or last insurer to have suffered at the hands of hackers. Just this summer, newsworthy hacks included a Canadian life insurer (internal email accounts of 10 employees compromised) and the Pittsburgh-based vendor of a health insurer (members' names, addresses, birthdates and other information). The plaintiff's bar is even upping the ante with new suits alleging that workers compensation insurers are hacking their own consumers' personal data. **NAIC's Cybersecurity Model Law** Meanwhile, insurance regulators have been busy at work devising measures to ensure the cybersecurity of consumer data possessed by insurers. To that end, the National Association of Insurance Commissioners (NAIC) cybersecurity task force has revised its draft model law governing insurers' handling of consumer data, which was originally released in March 2016. The newly revised insurance data security model law has been exposed for public comment until Sept. 16, 2016. There are significant changes in the revised draft, as reflected in the redline, from the version originally exposed in March. As stated in its preamble, the purpose and intent of the model law is to establish insurer standards for data security, investigation and breach

notification. The revised version creates a liability carve-out where insurers have employed adequate encryption of data, such that breach of such data does not constitute a "data breach" under the terms of the model law. See Section 3(c) (Definitions: "The term 'data breach' does not include the unauthorized acquisition, release or use of encrypted personal information if the encryption, process or key is not also acquired, released or used without authorization.") Likewise, the revised model law defines the "harm or inconvenience" to consumers that underlies the insurers' duties in such a way as to provide some potential protection to insurers in defending data breach claims, and particularly class actions, as it emphasizes a "reasonable likelihood of harm" standard, rather than some of the more nebulous "increased potential" or inchoate "harm" allegations that have been at the root of some data breach class actions, eliciting mixed results on standing challenges. To wit, under the revised model law:

1. Identity theft;
2. Fraudulent transactions on financial accounts rendered unusable, unreadable or indecipherable; or
3. Other misuse as defined

Id. at Section 3(e) (emphasis added). Generally, the revised model left unchanged the definition of "personal information," which includes the following:

1. A financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password or other personal identification information required to access the financial account; or

2. Information including: The first name or first initial and last name of a consumer in combination with:
    a. The consumer's nontruncated social security number;
    b. The consumer's driver's license number, passport number, military identification number, or other similar number issued on a government-issued document used to verify identity;
    c. A user name or email address, in combination with a password or security question and answer that would permit access to an online or financial account of the consumer;
    d. Biometric data of the consumer that would permit access to financial accounts of the consumer;
    e. Health. Any information of the consumer that the licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;
    f. The consumer's date of birth;
    g. Information that the consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family or household purposes from the licensee;
    h. Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family or household purposes between a licensee and the consumer;
    i. Information the licensee obtains about the consumer in connection with providing an insurance product or service used primarily for personal, family or household purposes to the consumer; or
    j. A list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using the information described in [Subparagraphs (Section 3H(2)(g) through (h), information provided to licensees]), that is not publicly available.
3. Any of the data elements identified in Section 3H(2)(a) through (f) when not in connection with the consumer's first name or initial and last name, if those elements would be sufficient to permit the fraudulent assumption of the consumer's identity or unauthorized access to an account of the consumer.
4. Any information or data except age or gender, that relates to:
    a. The past, present or future physical, mental or behavioral health or condition of a consumer;
    b. The provision of health care to a consumer; or
    c. Payment for the provision of health care to a consumer.

Id. at Section 3(h). The revised model also reflects attention to the differences in treatment of

insurers (and other licensees, such as agents) of different types and sizes and the different types of information they collect. It provides regulators with some flexibility in examining insurers and their cybersecurity programs, in requiring insurers to implement and maintain an information security program. Section 4 of the model law lays out the requirements in flexible terms: Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession, custody or control, each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information. The licensee shall document, on an ongoing basis, compliance with its information security program. Id. at Section 4. The revised model also scraps the old section 5, which related to duties before a data breach occurs, including duties to notify policyholders of the types of information collected and stored, and further refines the duties of an insurer in the case of a data breach, particularly where it involves a vendor. Id., Sections 5-6. The revised model adds further detail in the notification requirements section, regarding notification to the commissioner (in addition to affected consumers). Id., Section 6. Finally, the revised draft substantially alters the enforcement provisions, providing much greater flexibility to regulators in enforcing its provisions. The new model explicitly disavows any private right of action. It also notably alters the mandatory "shall" language in the prior draft which would have potentially required agency action in the event of any suspected violation of the law. Thus, under the revised model, such enforcement actions would be permissive, and within the discretion of the commissioner. The revised model also eliminates the prior draft's inclusion of sections detailing penalties, judicial review and individual remedies. Id. However, the revised model law may not mollify insurers who have expressed particular concerns about uniform notification laws. After the first iteration of the model law was exposed for comment, various changes were discussed at the NAIC's annual meeting. One important issue for insurers was expressed by the American Council of Life Insurers (ACLI), theAmerican Insurance Association, and America's Health Insurance Plans with regard to the notification requirements, which, in the prior draft did not supersede other state notification laws already in place. As ACLI noted, its member companies have "serious concerns" about additional notification requirements that do not supersede existing state laws, and noted that the prior version required an insurer to provide notice to 50 different state attorneys general and 50 different insurance commissioners. Id. at 37. The revised model law, however, does not fairly meet these concerns, as it maintains notification requirements to insurance commissioners, but does not contain any changes indicating that the notification requirements supersede other state notification laws, effectively leaving insurers with two sets of 50 different standards In sum, the revised model law continues to provide detailed consumer protection provisions, particularly given the new and varying types of information insurers are collecting, and it may give some comfort to insurers in that it scales back some of the penalty and enforcement provisions. But some fundamental problems that insurers have previously expressed, especially surrounding uniformity and the superseding of other state notification laws, remain in this draft. As noted above, the public comment period currently extends to Sept. 16, 2016. Insurers and others will no doubt anxiously await further changes in another revised version in the

hope that some of the as-yet addressed concerns are met. Republished with permission by Law360 (subscription required).

Authored By

John C. Pitblado