Bloomberg BNA

Daily Report for Executives™

Insurance Privacy

Authors Daniel Vinish and Ellen Farrell of Crowell & Moring outline the current state and federal regulatory frameworks that insurers must navigate in order to ensure adequate protection of non-public consumer information. And they take a close look at how the NAIC's recent efforts to standardize cybersecurity regulations might redefine the way in which insurance companies approach the whole issue. Conclusion: With its recently released ''Insurance Data Security Model Law,'' the NAIC is bidding to establish a one-stop source for the regulation of insurance companies' cybersecurity.

Cybersecurity and Consumer Data Privacy in the Insurance Sector: The Current Framework and a Look Ahead

BY DANIEL VINISH AND ELLEN FARRELL

As companies have increasingly moved to electronic storage media and as the vulnerability of that media has become more apparent, Congress and state legislatures have enacted numerous laws to help protect the privacy and security of confidential and personal consumer information. All states and the District of Columbia have now enacted laws specific to the insurance sector's use of confidential and personal consumer information. While these laws are largely based upon the National Association of Insurance Commissioners' (''NAIC'') Model Acts released in 1982, 1992, and 2002, states' insurance-specific laws vary in their treatment of consumer information and insurance companies often find themselves bound by other generally applicable state and federal laws as well.

At this point, the insurance-specific state laws arguably do not comprehensively address the obligations of insurance companies to ensure the privacy and security of consumer information. The NAIC has been working toward a solution to this issue since at least 2014, when the NAIC Executive Committee appointed a Cybersecurity Task Force (the ''Task Force'') ''to serve as the central focus for insurance regulatory activities related to cyber security.''[1] In April 2015, the Task Force adopted the Principles for Effective Cybersecurity Insurance Regulatory Guidance (the ''Cybersecurity Principles'') in order to set forth the NAIC's expectations for how insurance regulators and insurance companies alike will effectively protect the insurance sector's data security and infrastructure. Thereafter, in December 2015, the Task Force presented a Roadmap for Cybersecurity Consumer Protections (the ''Cybersecurity Roadmap'') (later adopted by the NAIC's Executive Committee and Plenary), which established a proposed ''Consumer Bill of Rights'' with respect to how insurance companies will secure and ensure the privacy of non-public consumer information. Neither the Cybersecurity Principles nor the Cybersecurity Roadmap, however, impose enforceable obligations on companies in the insurance sector.

Earlier this year, the Task Force followed the Cybersecurity Principles and Cybersecurity Roadmap with a proposed ''Insurance Data Security Model Law'' (the

Daniel Vinish *is counsel in Crowell & Moring's New York office.* **Ellen Farrell** *is senior counsel in Crowell & Moring's D.C. office. Both are members of the firm's Insurance/Reinsurance Group focusing on litigation and arbitration, as well as counseling on policy language, data privacy, and security issues.*

[1] *See* NAIC's Center for Insurance Policy and Research, *Cybersecurity*, *available at* http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last updated Jan. 25, 2016).

 ISSN 0148-8155

''2016 Model Law''). Unlike the Cybersecurity Principles and Cybersecurity Roadmap, the 2016 Model Act will, once finalized, provide a template for uniform, enforceable obligations for insurance companies with respect to cybersecurity. State insurance regulators will be able to adopt the 2016 Model Act or, at a minimum, use it to modify their existing regulatory frameworks.

This paper first discusses the current state and federal regulatory frameworks that insurers must navigate in order to ensure adequate protection of non-public consumer information. We then discuss in more detail the NAIC's recent efforts to standardize cybersecurity regulations, and how these efforts might redefine the way in which insurance companies approach the issue.

I. State Laws

A. Insurance-Specific Laws

The NAIC's first model acts to address the privacy of information in the insurance sector were the Insurance Information and Privacy Protection Model Act of 1982 (''1982 Model Act) and the Insurance Information and Privacy Protection Model Act of 1992 (''1992 Model Act'').[2] While the 1982 and 1992 Model Acts had aimed to standardize how insurance companies could collect, use, and disclose personal and confidential consumer information gathered in connection with insurance transactions, state adoption of them was not uniform, with only fifteen states ultimately adopting either the 1982 or 1992 Model Act.

Then, in 1999, Congress introduced the Gramm-Leach-Bliley Act (''GLBA'').[3] The GLBA established minimum security standards for the protection of consumers' non-public personal information and forced the insurance sector to rethink how it was addressing the privacy of consumer information. Under the GLBA, all ''financial institution[s]'' that provide financial products or services that are used primarily for ''personal, family or household purposes'' have an ''affirmative and continuing obligation to respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information.''[4]

The GLBA extends to insurance companies in respect of any financial products or services that are to be used for ''personal, family or household'' purposes.[5] (Conversely, the GLBA does not apply to information obtained or generated with respect to insurance issued to businesses.) However, since the McCarran-Ferguson Act largely exempts the business of insurance from federal regulation, states were left to enact legislation to implement the GLBA. The NAIC issued model legislation in the form of the Standards for Safeguarding Customer Information Model Regulation (the ''2002 Model Act'') expressly for this purpose.[6] Thirty-five states and the District of Columbia have adopted the 2002 Model Act, while other states chose to amend their existing regulatory frameworks to comply with the GLBA.

The 2002 Model Act requires governed entities to implement a comprehensive written Information Security Program (or ''ISP''), which outlines the entity's ''administrative, technical and physical safeguards'' for the protection of consumer information.[7] While the 2002 Model Act incorporated the GLBA's content requirements for ISPs[8], the 2002 Model Act also included examples on how insurers might assess, manage, and control their privacy risks, oversee their third-party service providers, and monitor and adjust their ISPs from time to time as needed.[9] With only a few exceptions, the states that adopted the 2002 Model Act explicitly incorporated a written ISP requirement and adopted the NAIC's examples for ensuring GLBA-compliance. (The 2002 Model Act does not expressly incorporate the GLBA's ''opt out'' procedures that bar disclosure of consumer information to unaffiliated third parties unless consumers are both notified in advance of the intended disclosure and provided an opportunity to ''opt out'' of the disclosure, but financial institutions subject to the GLBA must still follow this procedure.)

B. Data Security Laws Not Specific to the Insurance Sector

1. Pre-Breach Security Measure Laws

An increasing number of states today explicitly require some form of pre-breach security measures for protecting consumers' personal information. Generally, these states require reasonable practices, procedures, and/or safeguards to prevent unauthorized access, use, modification, and/or disclosure of this information.[10]

Recently, however, California's Attorney General effectively set a new standard for pre-breach security measures for most national insurers since, as a practical matter, the composition of a national insurer's customer base is likely to expose the insurer to California's privacy laws. On February 16, 2016, the California Attorney General issued a series of recommendations as part of its latest Data Breach Report that, among other things, caution all organizations subject to California law that a ''failure to implement all the [Center for Internet Security's Critical Security] Controls[11] [the ''CIS Controls''] that apply to an organization's environment constitutes a lack of reasonable security'' under California's personal information security statute.[12] As California's Attorney General has explained, the CIS Con-

[2] *See* Insurance Information and Privacy Protection Model Act of 1992, *available at* http://www.naic.org/store/free/MDL-670.pdf (last accessed Apr. 15, 2016).

[3] *See* Gramm-Leach-Bliley Act, 113 STAT. 1338 (codified at 15 U.S.C. § 6801, *et seq.*), *available at* https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (last accessed Apr. 15, 2016).

[4] *See* 15 U.S.C. § 6809(9) (emphasis added).

[5] *See* 15 U.S.C. § 6801, Sec. 501. For those engaged in providing insurance, ''the applicable State insurance authority of the State in which the person is domiciled, subject to § 6701 of this title'' enforces the requirements of the GLBA's Subtitle A. *See* 15 U.S.C. § 6805(a)(6).

[6] *See* Standards for Safeguarding Customer Information Model Regulation of 2002, *available at* http://www.naic.org/store/free/MDL-673.pdf (last accessed Apr. 15, 2016).

[7] *See id.*, § 1(A).

[8] *See* Standards for Safeguarding Customer Information, 16 C.F.R. 314.

[9] *See id.*, §§ 6-9.

[10] *See e.g.*, Cal. Civ. Code § 1798.81.5(b).

[11] *See* Center for Internet Security, CIS Critical Safety Controls, *available at* https://www.cisecurity.org/critical-controls.cfm (last accessed Apr. 14, 2016).

[12] *See* California Data Breach Report, Kamala D. Harris, Attorney General California Department of Justice, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf? (last accessed Apr. 14, 2016).

  DER ISSN 0148-8155

trols ''define a minimum level of information security that all organizations that collect or maintain personal information should meet.''[13]

2. Breach Notification Laws

Almost all states have enacted breach notification laws that require the disclosure of any data breach to any person whose personal information was involved in the breach.[14] Generally speaking, if it is a data owner, the organization subject to the security breach must notify all individuals potentially impacted by the data breach and provide certain services to those individuals (conversely, third-party vendors servicing data owners are required only to report to the data owner, whose obligations to notify potentially impacted individuals and provide related services would then arise). Many states provide an exception to this rule, however, if the information subject to the breach was encrypted at the time of breach, although some states have likewise recognized that this exception will not apply if the encryption keys have also been compromised. Other states have also provided exceptions for entities that are covered by and follow the notification procedures of the GLBA or other federal law.

The threshold trigger for notification is generally whether the data is reasonably believed to have been used, accessed, or acquired by an unauthorized person. All states require that this notification be accomplished without unreasonable delay and some states have likewise established outer boundaries by which notice must be given.[15] That said, many states have accepted the reality that over-notification may actually lead to a less secure economy and have therefore enacted ''harm triggers'' that, in effect, relieve entities of any obligation to notify affected individuals of data breaches where there is a low likelihood of identity theft or other financial harm to the consumer.

With little exception, nearly all state breach notification laws require a written notification that sets forth a general description of the unauthorized access to the recipient's personal information, yet the exact content of these notifications varies by state. In some instances, states have established substitute notice triggers as well. When met, these substitute notice triggers permit the entity to issue alternative notification methods that direct consumers to, for example, detailed notice of the breach on the organization's website and/or to statewide media advising of the breach. Some states similarly permit email as a regular form of notice, but most states require that the consumers pre-authorize such notice.

3. State Record Disposal Laws

State record disposal laws are intended to stop identity theft through the disposal of records (regardless of media) that might contain personal information by requiring that such records be rendered unreadable, indecipherable, illegible, or otherwise unusable.[16] These laws generally apply to businesses without regard to whether the records being disposed of contain personal information about a resident of the state; however, exemptions may apply, especially where an organization is subject to and in compliance with, for example, the GLBA or the Heath Insurance Portability and Accountability Act (''HIPAA''), as discussed more fully below.

State regulations vary here in terms of the extent to which organizations must ensure records are properly disposed of, with the majority of states approving ''reasonable'' measures. Some states have implemented much stricter guidelines that require organizations not only to implement and actively monitor policies that ensure secure destruction of all personal information, but similarly require due diligence over any third-party contractors engaged to assist in the destruction of any personal information.

4. State Laws Regarding the Protection of Social Security Numbers (''SSN'')

Many states have passed laws regarding the protection of individuals' SSNs to protect against identity theft.[17] Most of these laws require that an entity using SSNs in the ordinary course of business implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of personal information, including disposal of that SSN data. A majority of the states that have enacted these laws prohibit such things as intentionally making a SSN public, printing (and in some states, embedding electronically) a SSN on any card required to access products or services, requiring the use of a SSN to access a public website unless coupled with another unique authentication method (*e.g.*, password), and mailing any printed document containing a SSN unless explicitly authorized by law.

Most such laws apply to the use of an individual's SSN without regard to residency or the location of any data breach. While these laws are relatively absolute in their applicability, exceptions may apply in a particular state for, *inter alia*, compliance with the GLBA and/or HIPAA, ''grandfathered'' activities otherwise prohibited under state law, or the number of digits in the SSN that organizations must protect.

5. State Deceptive Trade Practice Acts

Many states have likewise enacted laws to emulate the Federal Trade Commission Act (discussed below) by imposing liability and fines for misleading or false statements by an organization about the level of information security policies that it has in place and, simi-

---

[13] *See id*, at p. 30, Recommendation 1.

[14] *See* National Conference of State Legislatures (''NCSL''), *Security Breach Notification Laws*, *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#2 (last updated Jan. 4, 2016).

[15] *See e.g.*, Fla. Stat. Ann. § 501.171 (requiring notice to the insurance department within 30 days of a breach of security affecting 500 or more individuals in the state).

[16] Under these laws, acceptable disposal methods can include the following: (1) burning, pulverizing, or shredding paper documents; (2) destroying or erasing non-paper media; (3) otherwise modifying records; or (4) redacting PI or removing PI from records. *See generally*, NCSL, *Data Disposal Laws*, *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx (last updated Jan. 12, 2016).

[17] *See e.g.*, NCSL, *Social Security Number 2009 Legislation*, *available at* http://www.ncsl.org/research/financial-services-and-commerce/social-security-number-2009-legislation.aspx (last updated May 7, 2010); NCSL, *Social Security Number 2010 Legislation*, *available at* http://www.ncsl.org/research/financial-services-and-commerce/social-security-number-2010-legislation.aspx (last updated June 21, 2010).

larly, the failure to reasonably secure data. Some states define violations of their pre-breach security measures, records disposal laws, and/or SSN protection laws as deceptive or unfair trade practices under these acts.

II. Federal Laws

In addition to state laws, insurance companies may also be subject to various federal statutes generally applicable to the use and disclosure of certain non-public personal information. These include the GLBA discussed above, as well as, among others, the Health Insurance Portability and Accountability Act (''HIPAA'') and the Federal Trade Commission Act (the ''FTC Act'').

A. HIPAA

HIPAA was designed to create minimum standards for the privacy and security of certain ''protected health information'' or ''PHI'' by regulating the activities of ''Covered Entities'' and related ''Business Associates.''[18] Covered Entities are health plans[19], healthcare clearinghouses[20], and health care providers[21], while the term Business Associates is defined more broadly to capture any entities that perform or assist a Covered Entity in operations involving the use or disclosure of PHI.

PHI includes any health information that is ''individually identifiable'' (meaning it identifies specific individuals or could be used to identify individuals) and transmitted or maintained in any form or medium.[22] HIPAA's Privacy Rule governs the permissible use and disclosure of PHI,[23] while HIPAA's Security Rule addresses the administrative, physical, and technical safeguards that Covered Entities and their Business Associates are required to have in place.[24] HIPAA also incorporates a Breach Notification Rule that requires notification to consumers when their unsecured PHI is subjected to unauthorized access, acquisition, use, or disclosure that compromises the security or privacy of the data.[25]

B. The FTC Act

Section 5 of the FTC Act prohibits unfair and deceptive commercial acts and practices.[26] The FTC exercises its enforcement authority where an organization uses or discloses consumer information in a way that is inconsistent with the organization's stated privacy policies or otherwise creates an unreasonable risk of harm to consumers by failing to adequately protect the security of their data. Privacy policies are ''deceptive'' under the FTC Act if they are likely to mislead consumers acting reasonably under the circumstances and affect their decisions with respect to the product or service at issue.[27] Similarly, conduct is ''unfair'' under the FTC Act if the injury it is likely to cause to consumers is substantial, is not reasonably avoidable by consumers themselves, and is not outweighed by countervailing benefits to consumers or to competition.[28]

III. Recent NAIC Actions

As noted, the NAIC's Cybersecurity Task Force has been taking steps to develop a uniform baseline for cybersecurity protection in the insurance sector. In 2015, these efforts culminated in the Task Force issuing new Cybersecurity Principles, aimed specifically at the actions of state insurance regulators and insurers/producers. The Task Force later followed with a Cybersecurity Roadmap specifically targeting consumers' rights in respect of their non-public personal information. Recently, in January 2016, the Task Force incorporated this guidance into a revised model law that state insurance regulators ultimately may be able to use to further secure consumer information. Each of these steps is discussed in turn below.

A. The Cybersecurity Principles

The first step came by way of the Task Force's adoption, on April 16, 2015, of the Cybersecurity Principles.[29] As the Task Force explained at that time, the Cybersecurity Principles reflected ever-increasing cybersecurity threats facing the insurance sector and the vital need for collaboration between state regulators and insurance sector participants to both identify and adequately safeguard against such threats.

The focus of the Cybersecurity Principles is two-fold. Nearly half of the Cybersecurity Principles are aimed at encouraging state insurance regulators to incorporate particular elements into their cybersecurity regulatory frameworks. The Cybersecurity Principles remind state insurance regulators of their responsibility to ensure adequate protection within the insurance sector of all personally identifiable information held by insurers, producers, and other regulated entities, as well as their third-party service providers.[30] The Cybersecurity Principles likewise recommend that state insurance regulators ensure their regulatory frameworks are flexible, scalable, practical, risk-based, and considerate of insurance sector resources, as well as consistent with other nationally recognized efforts to strengthen the overall U.S. economy's cybersecurity framework.[31] The Cybersecurity Principles further provide that state insurance regulators should create appropriate oversight policies, including as examples risk-based financial examinations and market conduct examinations specifically for the purpose of evaluating private efforts to control cy-

[18] *See* 45 C.F.R. § 160.103.

[19] *E.g.*, health insurance companies, health maintenance organizations (''HMO''), company health plans. *See* 45 CFR 160.103.

[20] Any entity that processes or facilitates the processing of nonstandard health information received from another entity. *See* 45 CFR § 160.103.

[21] *E.g.*, doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies whenever transmitting any health information in electronic form in connection with a covered transaction. *See* 45 CFR § 160.103.

[22] *See* 45 C.F.R. § 160.103. HIPAA also regulates the use and disclosure of health information that does not identify specific individuals, but different rules and regulations apply.

[23] *See* 45 C.F.R. §§ 164.500 *et seq.*

[24] *See* 45 C.F.R. §§ 164.302 *et seq.*

[25] *See* 45 C.F.R. §§ 164.400 *et seq.*

[26] *See* 15 U.S.C.A. § 45.

[27] *See e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 627-29 (D.N.J. 2014).

[28] *See* 15 U.S.C.A. § 45 (n).

[29] *See* Cybersecurity Principles, *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf (last accessed Apr. 15, 2016).

[30] *See id.*, Principles 1-3.

[31] *See id.*, Principles 4-5.

  DER ISSN 0148-8155

bersecurity and data privacy threats within the industry.[32]

The remaining Cybersecurity Principles target the efforts of insurers, producers, and other regulated entities operating within the insurance sector to develop appropriate internal cybersecurity policies relative to the risks in the market. The Cybersecurity Principles encourage companies to incorporate cybersecurity into their enterprise risk management processes, recognizing that cybersecurity is not limited to a single, discreet function of any one company.[33] The Cybersecurity Principles similarly encourage insurance sector participants to adequately plan for incident response, provide periodic cybersecurity training for employees, conduct internal cybersecurity audits, advise their boards of directors of any material threats, and establish policies to ensure that third-party service providers are similarly cognizant of cybersecurity and data privacy.[34] The Cybersecurity Principles also acknowledge the important role that information-sharing and analysis organizations (''ISAOs'') could serve in the insurance sector.[35]

B. The Cybersecurity Roadmap

Shortly after adopting the Cybersecurity Principles discussed above, the Task Force issued the Cybersecurity Roadmap.[36] As explained by the Task Force, the Cybersecurity Roadmap is intended to serve as a ''Consumer Bill of Rights'' by outlining six protections consumers should be able to expect from their insurers to protect consumers from a cybersecurity breach. (At the same time, the Task Force recognized that not all state regulatory frameworks afforded consumers these protections and, as a result, indicated that the insurance sector should view the Cybersecurity Roadmap as a preview of the NAIC's next model law, discussed below.)

The protections afforded to consumers in the Cybersecurity Roadmap focus on establishing transparency for consumers as to the types of personal information collected and stored by insurers, and steps taken by insurers to keep this information secure from any unauthorized access.[37] Thus, a consumer has a right under the Cybersecurity Roadmap to receive a copy of his or her insurer's privacy policy,[38] and in the event of a breach the consumer should also receive the following: (1) written notice within a ''reasonable time thereafter''; (2) a description of the ''remedial actions'' the insurer plans on taking to keep the consumers' data safe; (3) contact information for the entity subject to the breach; (4) contact information for nationwide credit reporting bureaus; and (5) one year of identity theft protection paid for by the entity subject to the breach.[39] The Cybersecurity Roadmap also establishes a credit protection framework to aid consumers so affected.[40]

C. The 2016 Model Law

Against the backdrop of the Cybersecurity Principles and Cybersecurity Roadmap, on March 2, 2016, the Task Force unveiled the 2016 Model Law.[41] The express purpose of this new model law is to establish ''the exclusive standards'' for data security and the investigation and notification of any breach of data security for any state to adopt the model.[42] The NAIC has made clear by its explicit reference of the McCarran-Ferguson Act (which would allow the model law, if adopted, to preempt otherwise applicable state and federal law) that the NAIC intends for the 2016 Model Law to comprise one-stop shopping for the regulation of insurance companies' cybersecurity infrastructures.

The scope of the 2016 Model Law is broadly defined both in terms of the entities that would be subject to its regulations if adopted, as well as in terms of the personal information it protects. The new model law applies to all licensed insurers and producers, as well as to a new category of ''other persons'' required to be licensed, authorized, or registered under state law, potentially signaling flexibility for state regulators to increase the scope of the law through state legislation.[43] The new model law also imposes an obligation on these entities to require by contract that all third-party service providers maintain similar safeguards for the protection of consumers' personal information, notify the insurers/producers of any data breaches, indemnify insurers/producers in the event of any cybersecurity incident that results in a loss, allow insurers/producers to perform periodic cybersecurity audits, and represent and warrant their compliance with all of the model law's requirements.[44]

The rules outlined in the 2016 Model Law apply to a variety of financial, health, and other non-public personally identifiable information, which the NAIC has incorporated into a new multi-part definition of protected ''Personal Information.''[45] The definition also extends, *inter alia*, to cover any personally identifying information that a consumer provides in an effort to obtain or in connection with an insurer/producer's performance in respect of any insurance product or service primarily for personal, family, or household use.[46]

In terms of the controls mandated by the new model law, insurers/producers remain required to have in place an ISP, but ISPs must now (i) ensure the security and confidentiality of protected ''Personal Information''; (ii) protect against any threats or hazards to the security or integrity of protected ''Personal Information''; and (iii) protect against unauthorized access to, and use of, any protected ''Personal Information'' that

---

[32] *See id.*, Principle 6.
[33] *See id.*, Principle 9.
[34] *See id.*, Principles 7, 8, 10, and 12.
[35] *See id.*, Principle 11. The NAIC's efforts to have the insurance sector adopt the use of ISAOs mirrored the Executive Order President Obama signed into law just a few months earlier in February 2015, titled ''Promoting Private Sector Cybersecurity Information Sharing.'' *See* Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 13, 2015), *available at* http://tinyurl.com/kmrfuaq. At its core, this Executive Order directed the Department of Homeland Security to encourage the development and use of ISAOs at large in the U.S. economy.
[36] *See* Cybersecurity Roadmap, *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf (last accessed Apr. 15, 2016).
[37] *See id.*, Rights 1-3.
[38] See *id.*
[39] *See id.*, Rights 4-5.
[40] *See id.*, Right 6.
[41] *See* 2016 Model Law, *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_exposure_draft_insurance_data_sec_mdl_law.pdf (last accessed Apr. 15, 2016).
[42] *See id.*, at, § 1.
[43] *See id.*, at § 3(F).
[44] *See id.*, at § 4(G)(2).
[45] *See id.*, at § 3(G).
[46] *See id.*, at § 3(G).

could result in substantial harm or inconvenience to any customer.[47] ISPs must be appropriate in scale and scope to the size and complexity of the insurer/producer, the nature and scope of the insurer/producer's activities, and the sensitivity of the ''Personal Information'' in the insurer/producer's possession.[48]

The 2016 Model Law similarly requires that all ISPs contain a host of new security measures. These include placing access controls on information systems, restricting access to physical locations, encrypting electronic personal information, implementing multi-factor authentication procedures, regularly testing and monitoring systems in order to detect actual and attempted intrusions, implementing response programs, implementing policies and procedures for ensuring that personal information is not compromised in the event of a natural disaster, and implementing proper disposal methods for personal information, among others.[49] Insurers/producers are similarly required under the new model law to integrate cybersecurity into their enterprise risk management processes and to use ISAOs to stay informed regarding emerging cybersecurity threats.[50]

Consumers will also be entitled under the new model law to receive prior to any security breach, notice regarding the types of personal information collected and stored both by their insurers and by any third-party service providers assisting their insurers.[51] Insurers/producers are also required under the new model law to post their privacy policies on their websites, as well as make the policies available to consumers in hard copy upon request. These policies must advise consumers of (i) the personal information that was collected, (ii) all options consumers have about their data, (iii) how consumers can review and change/correct their data if needed, (iv) how data is stored and protected, and (v) what consumers can do if their insurer does not follow its privacy policy.[52]

To deal with the inevitability of a breach, the 2016 Model Law also establishes incident investigation requirements and a detailed consumer notification process. The new model law requires insurers/producers to conduct an investigation any time they believe their data security ''has or may have been'' breached in a way that subjected consumer's personal information to unauthorized access.[53] To the extent that insurers/producers determine that a consumer's personal information was acquired through a data breach, insurers/producers must notify not only the affected consumers, but also state commissioners of insurance and in certain circumstances, nationwide credit reporting agencies.[54] The 2016 Model Law, however, adopts a harm trigger similar to that which currently exists in many states across the country that relieves insurers/producers of providing this notice if the data security breach is not ''reasonably likely to cause substantial harm or inconvenience to the consumers to whom the information relates.''[55] The required notification to consumers largely mirrors the Cybersecurity Roadmap that the NAIC adopted in 2015.[56]

Additionally, the 2016 Model Law empowers state insurance commissioners to examine and investigate the operations of the insurers/producers in order to determine whether they are currently engaged in or have previously been engaged in any conduct in violation of the model law.[57] Where violations are determined to exist, the insurance commissioner will serve his or her written findings on the insurer/producer, along with a cease and desist order to stop the violating conduct.[58] The NAIC has further empowered the state insurance commissioners to levy monetary penalties up to a suggested per-violation fine of $500, with a suggested aggregate cap of $10,000.[59] A private cause of action for equitable relief against insurers/producers also exists for alleged violations of consumers' rights.[60]

IV. Conclusion

While it remains to be seen how states will react, the Task Force's current draft of the 2016 Model Law provides an extensive regulatory framework aimed specifically at ensuring adequate security measures across the insurance sector and imposing penalties upon insurers/producers where they fail to comply with these measures. The framework established by this new model law is notably more robust than the NAIC's prior statements in 1982, 1992, and 2002 in terms of cybersecurity, yet the model still remains a draft at this point. With the official window for public comment having closed on March 23, 2016, the insurance industry can expect the Task Force to analyze the assortment of comments it received as drafting continues. To the extent that the Task Force is able to satisfy the industry's concerns, it is possible that a new model law from the NAIC may help to alleviate insurers/producers of the burden of complying with the complicated sea of state and federal regulations that exists today.

[47] *See id.*, at § 4.
[48] *See id.*, at § 4.
[49] *See id.*, at § 4(E)(1).
[50] *See id.*, at § 4(E)(2) & (3).
[51] *See id.*, at § 5.
[52] *See id.*, at § 5.
[53] *See id.*, at § 6.
[54] *See id.*, at § 6.
[55] *See id.*, at § 7.
[56] *See id.*, at § 7.
[57] *See id.*, at § 9.
[58] *See id.*, at §§ 9-12.
[59] *See id.*, at § 13.
[60] *See id.*, at § 15.

  DER ISSN 0148-8155