Journal of Reinsurance 2020

Volume 27
Number 1

In This Issue:

Data Protection: Harmonizing Tensions Between the NAIC's "Insurance Data Security Law" & Traditional Access-To-Records Provisions

BY MATTHEW J. LASKY

About the Author:

Matthew J. Lasky is a partner with Mound Cotton Wollan & Greengrass LLP and has more than twenty years of experience in reinsurance, insurance, product liability, and commercial litigation and arbitration. He has participated in numerous reinsurance litigations and arbitrations, pending in various jurisdictions throughout the United States.

Mr. Lasky is a graduate of The Catholic University of America, where he received his B.A. in English and Political Science. He also received his J.D. (magna cum laude) from The Catholic University of America, Columbus School of Law, where he served as an Editorial Assistant for The Catholic University Law Review. Mr. Lasky is admitted to the New York, New Jersey and several federal bars.

Abstract:

The exchange of personal and business information is the (re)insurance industry's lifeblood: it is necessary to facilitate accurate and profitable underwriting, proper claims management, and the fulfillment of legal and/or regulatory obligations. Insurers and reinsurers share information with a wide variety of third-parties including brokers, claims administrators, auditors, retrocessionaires, and legal advisors. In a world where data breaches and cyber-attacks have become widespread, the protection of confidential information, as well as the minimization of cybersecurity risks, is a preeminent concern for the industry and the public at large.

Towards that end, a jumbled set of federal, state, and international laws have been implemented to try to protect private information utilized by businesses, as well as the systems employed to collect, process, store, and exchange such information. To address the cybersecurity risks that face the (re) insurance industry, the National Association of Insurance Commissioners (NAIC) adopted the "Insurance Data Security Model Law" (Model Law) in October 2017.[1] While the Model Law's stated purpose is to establish industry standards for data security and the investigation and reporting of cybersecurity events to state insurance commissioners,[2] these standards are sometimes difficult to reconcile with traditional reinsurance norms and access-to-records clauses. This article provides a brief overview of the Model Law and scrutinizes traditional reinsurance relationships in the face this new data protection regulatory scheme.

GENERAL PARAMETERS OF THE MODEL LAW

As of October 1, 2019, eight states have enacted a version of the Model Law: Alabama, Connecticut, Delaware, Michigan, Mississippi, New Hampshire, Ohio, and South Carolina (although based on staggered implementation periods, only South Carolina has compliance obligations that are currently in force).[3] In addition, compliance with New York's "Cybersecurity Requirements for Financial Services Companies" constitutes compliance with the Model Law.[4]

The Model Law contains its own enforcement mechanisms for any violation of its regulations: "a Licensee may be penalized in accordance with [*insert general penalty statute*]."[5] The regulations further provide the adopting state's insurance commissioner with broad powers to take action "as shall be necessary to carry out the provisions of this Act."[6]

With certain exceptions, the Model Law applies to all "Licensees," which are defined as "any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a **Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction**."[7] As the highlighted language indicates, a reinsurer domiciled in a foreign state or jurisdiction (i.e., has its home office elsewhere) is not subject to the Model Law.[8] So, for example, a reinsurer domiciled in Bermuda but "acting as" a reinsurer in South Carolina is not subject to South Carolina's data protection regulations based on the Model Law. A reinsurer domiciled in South Carolina, however, is subject to South Carolina's regulatory scheme.

Continued on page 4

Continued from page 3

ENSURING COMPLIANCE WITH THE MODEL LAW'S RISK ASSESSMENT & MANAGEMENT OBLIGATIONS THROUGH CONTRACTUAL SOLUTIONS

The backbone of the Model law is the requirement that all Licensees (with certain exceptions) develop, implement, and maintain a comprehensive "Information Security Program."[9] That Program must include administrative, technical, and physical safeguards[10] that protect (i) "Nonpublic Information"[11] (broadly defined to include all manner of personal and health information and certain business information) and (ii) "Information Systems" (e.g., processing systems, telephone switching, private branch exchange systems, etc.[12]).

Development of the Program is based on a Licensee's self-risk assessment that identifies reasonably foreseeable threats to the data and systems of both Licensees and their third-party service providers.[13] "Third-Party Service Providers," in turn, are defined as: "a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee."[14] Licensees have further data protection oversight obligations related to the use of Third-Party Service Providers (i.e., consultants, outside auditors, discovery vendors, attorneys etc.), including conducting due diligence in selecting such service providers and requiring them to implement their own appropriate data protection safeguards.[15]

These risk assessment and management obligations raise potential problems under traditional reinsurance access-to-records clauses, e.g.: "The Reinsurers or their designated representatives shall have free access at any reasonable time to all records of the Reinsured which pertain in any way to this Agreement." On its face, such a provision has no safeguards in place to mitigate against data hacking, which could leave a cedent (or domiciliary reinsurer) in peril under the Model Law.

Take for instance a classic reinsurance audit fact pattern. A non-domiciliary reinsurer invokes its access-to-records rights under the above clause. The reinsurer then hires unscreened outside auditors to conduct an "unfettered" inspection. As part of the review, the reinsurer demands that sensitive data be copied by outside vendors and produced electronically. Potential Model Law violations may arise in such a scenario, such as:

- The auditors use a corrupted flash drive that disrupts the cedent's data systems or the auditors gain unauthorized access to restricted information.
- The vendors leave sensitive information unguarded during the copying process.
- During the electronic exchange of information with the reinsurer, the cedent sends unencrypted data by email that is intercepted by hackers.

To mitigate the chances of Model Law violations, reinsurance contracts should be carefully tailored to include data protection clauses setting forth appropriate practices and procedures for the inspection and exchange of information, such as the following sample language proposed by the AIDA Reinsurance and Insurance Arbitration Society ("ARIAS"):

> The parties have agreed to use the following reasonable methods to protect the data and other information [exchanged under this contract] from cyber breaches [*insert mandated use of cyber protection software, encryption and other relevant procedures*]. Any breach or loss of data as a result of a cyber breach shall be reported to the other party(ies) [within 72 hours of discovery], so that appropriate remediation measures may be undertaken.[16]

The Brokers & Reinsurance Market Association (BRMA) has also suggested contract language that mandates compliance with the data protection regulations to close any potential safeguard holes:

> A. The Company and the Reinsurer represent that they are aware of and in compliance with their responsibilities and obligations under [the NAIC's model Insurance Data Security Law (hereinafter "Model Law")]. For the purpose of this Contract, ["Nonpublic Information"] shall mean [personal], financial, or health information that identifies an individual, including claimants under Policies reinsured under this Contract, and which information is not otherwise available to the public. Data conveyed through the Intermediary may include [Nonpublic Information] that is protected under applicable laws and regulations and shall be used only in the performance of rights, obligations and duties in connection with this Contract.
>
> B. The Intermediary shall receive and convey [Nonpublic Information] that it has received from the parties to this Contract or others for the sole purpose of carrying out the respective obligations of the parties under this Contract. To the extent that this Contract is placed in conjunction with one or more corresponding Intermediaries the parties hereby authorize the transmission of the relevant data through the corresponding Intermediaries whether located in the United States or any other country. The parties shall use any [Nonpublic Information] received from another party or the Intermediary only as may be necessary to satisfy their respective obligations under this Contract. Furthermore, the parties shall maintain appropriate safeguards to protect any data received from accidental loss or unauthorized access, use or disclosure [in accordance with the Model Law].[17]

To further ensure compliance with the Model Law, consideration should be given to reinsurance contract language that (i) limits records inspections to individuals with pre-determined qualifications so as to minimize the chances of a data breach and (ii) requires the use of pre-approved vendors that have their own appropriate administrative, technical, and physical measures in place to protect sensitive data.

THE MODEL LAW'S INVESTIGATION & NOTIFICATION OBLIGATIONS SHOULD ALSO BE ADDRESSED WITH UPDATED REINSURANCE CONTRACT LANGUAGE

The Model Law also requires Licensees to promptly investigate and remediate actual or potential "Cybersecurity Events," which are defined as events resulting in unauthorized access to, disruption, or misuse of an Information System or information stored on an Information System (with certain exceptions).[18] Licensees additionally have a duty to ensure that the same investigations take place for any potential Cybersecurity Events that affect the systems of their Third Party Service Providers.[19] So it is a best practice within the industry to ensure that any contracts with such service providers (i.e., consultants, vendors, legal advisors) contain provisions that require appropriate investigations and remedies for potential or actual Cybersecurity Events.

Once a Cybersecurity Event has been determined to occur, within 72 hours the Licensee must provide notice to the insurance commissioner in the Licensee's state of domicile and, with certain exceptions, to the insurance commissioner of another state where the Licensee reasonably believes that the Cybersecurity Event affects the nonpublic information of 250 or more consumers residing in that state.[20] While there is no independent obligation under the Model Law to notify consumers of Cybersecurity Events, the

Licensee is required to comply with an applicable state's breach notification laws, and to provide a copy of notices under such laws to the insurance commissioners of the implicated states.[21] For Cybersecurity Events involving Third-Party Service Providers, the Model Law requires Licensees to treat such events as their own and follow the above notification rules.[22]

The Model Law also has specific notification provisions for domiciliaries acting as assuming insurers.[23] Once a Cybersecurity Event related to such a reinsurer or its service providers has been determined to occur, within 72 hours those reinsurers generally must provide notice to its cedents and the insurance commissioner in the reinsurer's state of domicile.[24] The cedent is then required to fulfill the same notification requirements as if the data breach were its own.[25] There are, however, no provisions in the Model Law addressing data breaches for non-domiciliary reinsurers or their service providers. As discussed *supra*, that is because non-domiciliary reinsurers are not Licensees to whom the Model Law applies. That may leave a cedent in the dark if a breach of its non-domiciliary reinsurer's data system takes place. Consideration should therefore be given to reinsurance contract language that requires non-domiciliary reinsurers to comply with the Model Law to close any data protection holes.

CONCLUSION

The Model Law is not the only data protection regulatory scheme that may affect the business of a cedent or reinsurer. Parties should always investigate and determine whether any other data protection regulatory schemes apply to their business, and draft their reinsurance contracts accordingly. Nonetheless, full compliance with the Model Law may do more than simply avoid monetary and other statutory penalties under that regulatory scheme. It could also demonstrate that parties to a reinsurance contract acted with the appropriate standard of care if a data breach were to eventually occur. As one commentator put it:

> In other words, if the defendant business can show *complete* compliance with the Model Law, then the court should find that the business acted reasonably under the circumstances. By making the Model Law an industry standard and requiring *complete* compliance, businesses would have a clear view of exactly what would be required of them with respect to cybersecurity. Most importantly, customers would have the greatest assurance that companies are incentivized to protect their information. Companies are less apt to cut corners knowing that there is a realistic way to protect themselves from liability. Currently, companies have no such assurance. But, through the use of the Model Law as the standard of care, companies would be aware that a [data] breach would not automatically result in insurmountable liability so long as the breach was one that even a Model Law-complaint cybersecurity program could not stop.[26]

The potential for courts and panels to use the Model law as the appropriate standard of care for data protection in the (re)insurance industry is all the more reason to carefully craft reinsurance contracts to ensure that all parties that play a role in the reinsurance relationship are Model Law compliant. ◀

1 NAIC Insurance Data Security Model Law (4th Quarter 2017), available at https://content.naic.org/sites/default/files/inline-files/cmte_ex_cswg_related_ins_data_security_model.pdf.

2 *See id.*, at Section 2.

3 Mark Smith, ANALYSIS: *Data Security Mandates Expanding for Insurance Sector,* BLOOMBERG LAW (Sept. 17, 2019), *available at* https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-data-security-mandates-expanding-for-insurance-sector.

4 *See* n. 1, *supra*, at Section 2, Drafting Note.

5 *See id*., at Section 10 (the governing state's applicable penalty statute should be inserted here).

6 *See id.*, at Section 11.

7 *See id.*, at Section 3(I) (emphases added).

8 The Model Law does not define "domicile." "State of Domicile" is defined as "the state where a company's home office is located" in the NAIC's *Glossary of Insurance Terms available at* https://www.naic.org/consumer_glossary.htm.

9 Theodore P. Augustinos, *A Closer Look at the NAIC Insurance Data Security Model Law,* LOCKE LORD INSURANCE & REINSURANCE NEWSLETTER (April 2018), *available at* https://www.lockelord.com/newsandevents/publications/2018/04/~/media/D517F16B7BD947CBAC5DDCDE15B12049.ashx.

10 *See* n. 1, *supra*, at Section 4(A).

11 *Id.*, at Section 3(K).

12 *Id.*, at Section 3(H).

13 *See id*., at Section 4(C).

14 *Id*., at Section 3(P).

15 *See id*., at Section 4(F).

16 ARIAS U.S. Sample Form 3.3 – Confidentiality Agreement, paragraph 6, *available at* https://www.arias-us.org/arias-us-dispute-resolution-process/forms/ (the parties' agreed upon procedures to protect data and other information should be incorporated into this provision).

17 Brokers & Reinsurance Market Association, Contract Wording, Privacy & Protection of Data Sample Form 77A (Fall 2018), *available at* https://brma.org/contract_wording.php.

18 *See* n. 1, *supra,* at Sections 3(D) and 5.

19 *See id*., at Section 5(C).

20 *See id*., at Section 6(A).

21 *See id*., at Section 6(C).

22 *See id*., at Section 6(D).

23 *See id*., at Section 6(E).

24 *See id*.

25 *See id*.

26 Koyejo-Isaac Idowu, *The Insurance Data Security Model Law: Strengthening Cybersecurity Insurer-Policyholder Relationships and Protecting Consumers*, 24 ROGER WILLIAMS U.L. REV. 115 at 135-136 (2019) (emphases in original).

Intermediaries & Reinsurance Underwriters Association / Board of Directors

Officers

President
Andrew L. Downing
RFIB Americas

1st Vice President
Laura Herubin
Mapfre Re, N. America

2nd Vice President
William Bernens
Arch Re

Secretary
Tim Poeton
State National Companies

Treasurer
Christiane Gross
Munich Reinsurance Americas, Inc.

Immediate Past President
Arlene S. Kern
Munich Reinsurance America, Inc.

Directors

Dawnmarie Black
Lloyd's America, Inc.

Paul Carroll
Markel Global Re

Keth Cartmell
Sirius America Re Managers

Nick Cook
Crum & Forster

Sam DeGiovanni
Aspen Re

Dwayne E. Elliott
American Agricultural Insurance Company

James D. Fletcher
Odyssey Reinsurance

Joshua Hackett
Arch Reinsurance Company

Thomas Hettinger
Guy Carpenter & Company, LLC

Danny Hojnowski
Transatlantic Reinsurance Company

Julie A. McLoughlin
Guy Carpenter & Company, LLC

James P. McNally
Toa Reinsurance Company of America

Kevin Rentko
Renaissance Re US

Michael Schummer
Munich Reinsurance America, Inc.

Michael C. Sowa
Aspen Re

Roderick P. Thaler
Holborn Corporation

John West
Apetrop USA, Inc.

James Wilson
Partner Re US

Staff

Executive Director
Jeremy Wallis
Jeremy R. Wallis Reinsurance Consulting & Arbitration Services

Counsel
Robert Calinoff
Calinoff & Katz, LLP

Executive Administrator
Maria Sclafani
The Beaumont Group, Inc.

Journal of Reinsurance Committee

Duane Hynes
Holborn Corporation

Mike Kurtis
Trans Re

Daniel Sheehan
Everest Re

John West
Apetrop USA, Inc.

Journal of Reinsurance Industry Advisory Panel

Fred Pomerantz
Ins. Legal & Regulatory Consulting

Susan E. Mack
Adams & Reese, LLP

Lloyd A. Gura
Mound Cotton Wollan & Greengrass LLP

M. Michael Zuckerman, J.D.
Temple University

Vision

To facilitate a vibrant forum that encourages professional and personal development of member company personnel through educational excellence, the exchange of knowledge among industry constituents within the insurance and reinsurance marketplace and recognition for academic excellence for the next generation of reinsurance professionals. We accomplish this vision through focused educational offerings, a robust Scholars program, the publication of the *Journal of Reinsurance,* and an Annual Conference.

Mission Statement

The IRUA is a not-for-profit corporation, organized for the purpose of providing high-quality insurance and reinsurance education, meaningful networking opportunities, and the dissemination of topical publications and information relevant to the reinsurance industry.

Disclaimer

The *Journal of Reinsurance* is published by IRU Inc.© 2019. All rights reserved. No reproduction of any portion of this issue is allowed without the publisher's prior written permission. All opinions and views expressed in any material in the *Journal of Reinsurance* are those of the author(s) and do not necessarily represent the views of the IRU, Inc. its agents or its members. IRU Inc. does not edit original content and accepts no responsibility for the accuracy of any statement, comment or view expressed therein. Copyright© IRU, Inc. All rights reserved. ISSN 1074-2948.