ALSTON&BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

JUNE 13, 2016

Insurers Face Increasing Data Breach Notice Obligations

by Jim Harvey and Bruce Sarkisian

Earlier this year, the National Association of Insurance Commissioners' (NAIC) Cybersecurity Task Force proposed a comprehensive model law[1] that covers, among other things, data security breach reporting. The model law followed closely on the heels of the NAIC Task Force's adoption of a "Cybersecurity Bill of Rights,"[2] which outlines the rights that the task force believes consumers should expect when they entrust their personal information to an insurance company. In late May, the Cybersecurity Task Force met again to discuss comments from the insurance industry on the model law (including the notification requirements), but no changes have yet been made to the model law as a result.

This level of focus reflects cybersecurity events in the insurance and financial services spaces and throughout the broader business community. While some may argue that the issue deserves more attention within the insurance industry, the requirements of the model law would impose a set of data breach reporting requirements on insurers that is significantly more demanding than existing state and federal law on breach notification.

Recent Breaches Increase Industry Scrutiny

Recent data breaches targeting the insurance industry have shown that cyber criminals are no longer limiting their targets to information that can quickly be monetized, such as credit card information. Hackers are increasingly looking to assemble comprehensive data portfolios on their victims that can be used to commit more lucrative, and troubling, forms of identity theft. In January 2015, Anthem Inc. disclosed that nearly 80 million current and former members of its affiliated health plans in several states may have been impacted by a cyberattack on its systems. The information that was potentially accessed may have included Social Security numbers and health care ID numbers. Later in 2015, several other insurers disclosed similar

---

1 *See* "Insurance Data Security Model Law" (the "NAIC Model Law") *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_160524_draft_ins_data_sec_model_law.pdf.

2 *See* "NAIC Roadmap for Cybersecurity Consumer Protections" *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf.

cyber intrusions affecting tens of millions of consumers, including Excellus Health Plan in New York, Premera Blue Cross Blue Shield in Washington and the UCLA Health System.

Depending on the breadth of their portfolios, insurance companies have a wide range of data on individuals from health history to financial data (including credit, payment card and bank account information) to driving history. Anthem and the other industry events serve as a reminder that cyber criminals and, perhaps, nation-state attackers have realized that insurance companies typically store and process significant amounts of personal data from which the attackers may benefit.

Existing and Proposed Data Breach Notification Requirements

Straddling a number of different sectors, insurers face a unique regulatory landscape because of the breadth of sectoral laws they are subject to, such as HIPAA and the Gramm-Leach-Bliley Act. Additionally, just like every other company in the U.S., insurers are already subject to the more than 47 state and territorial laws on data breach notification, and each state insurance commissioner can impose cybersecurity breach reporting requirements on the insurance companies they regulate. Several state commissioners already have done so, including in California,[3] Maine,[4] Montana,[5] Ohio,[6] Rhode Island,[7] Vermont,[8] Washington[9] and Wisconsin.[10]

The NAIC model law includes some of the most comprehensive and stringent data breach notification requirements of all of the notification regimes an insurer may be subject to. For example, the NAIC model law requires an insurer to notify law enforcement,[11] the state insurance commissioner,[12] payment card networks (if applicable),[13] credit reporting agencies (if the breach affects more than 1,000 consumers)[14] and the individual consumers themselves.[15] While many companies do notify law enforcement following a data breach because they would like their assistance in pursuing the cyber criminals, a requirement to notify "an

---

3 California Department of Insurance Notice dated May 16, 2014, *available at*: http://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/NoticeToInsurersDataBreachReq.pdf.

4 Maine Bureau of Insurance Bulletin 345, *available at*: http://www.maine.gov/pfr/insurance/bulletins/345.htm.

5 Mont. Code. Ann. §33-19-321(5).

6 Ohio Insurance Department Bulletin 2009-12, *available at:* https://insurance.ohio.gov/Legal/Bulletins/Documents/2009-12.pdf.

7 Rhode Island Insurance Regulation 107, *available at*: http://www.dbr.state.ri.us/documents/rules/insurance/InsuranceRegulation107.pdf.

8 Vermont Department of Financial Regulation DFR Bulletin Number 3 effective May 13, 2013, *available at*: http://www.dfr.vermont.gov/sites/default/files/DFR%20Bulletin%20Number%203.pdf.

9 Wash. Rev. Code §284-04-625, *available at*: http://apps.leg.wa.gov/wac/default.aspx?cite=284-04-625.

10 Wisconsin Office of the Commissioner of Insurance, Bulletin to Insurers dated December 4, 2006, *available at*: http://oci.wi.gov/bulletin/1206security.htm.

11 NAIC Model Law at Section 7.A(1).

12 *Id*. at Section 7.A(2).

13 *Id*. at Section 7.A(3).

14 *Id*. at Section 7.A(4).

15 *Id*. at Section 7.A(5).

appropriate federal and state law enforcement agency" is not generally required by other statutes. Similarly, companies are required via the payment card brand rules to notify the payment card networks of a breach involving card information, but there is no current statutory requirement to do so.

The law also specifies that the state insurance commissioner must be notified within five days after "identifying the breach."[16] The short time requirement is likely to cause many insurers anxiety about disclosing an event outside the company before relevant facts can be known with sufficient certainty. The five-day notice requirement will not be unfamiliar to insurers doing business in Connecticut, as that state's insurance commissioner imposed this requirement in 2010.[17] In addition, when notifying the insurance commissioner of a breach under the model law, a company must also provide a copy of its privacy and data breach policies (which is a novel requirement in and of itself). If those policies are nonexistent or not sophisticated, regulators may show even more interest and add yet another area of discomfort for an insurer.[18]

Under the NAIC model law, consumers must be notified within 60 days after the company identifies the data breach.[19] Before notice is provided to consumers, the company must provide its proposed consumer notification to the state insurance commissioner (no later than 45 days after the breach is identified), and the commissioner has the right to edit the company's notification letter.[20] In addition, companies must offer "appropriate identity theft protection services" without cost to the consumer for a minimum of 12 months.[21] Although it has become commonplace for companies that are breached to offer credit monitoring or identity theft protection, the only state currently requiring such protection is Connecticut,[22] which implemented the requirement in 2015. Additionally, California requires any company choosing to offer identity theft protection following a breach to provide the protection to affected individuals at no cost for at least 12 months.[23]

Still more data breach regulation may be on the horizon. In the wake of two breaches of its database in 2015 that exposed the personal information of 21.5 million government employees and applicants, the Office of Personnel Management (OPM) announced at a carrier conference on March 31, 2016, that it will provide new rules to government employee health insurers regarding data breach notices. When announcing the forthcoming rules, acting OPM director Beth Cobert said they would attempt to ensure that the insurance companies' policies "are complete, sufficient, and uniform when it comes to reporting data breaches and that, going forward, carrier practices are aligned with best practices in IT."[24]

---

16 *Id*. at Section 7.B.

17 Please see State of Connecticut Insurance Department Bulletin IC-25 (August 18, 2010).

18 NAIC Model Law at Section 7.B(13).

19 *Id*. at Section 7.D(1).

20 *Id*. at Section 7.D(3).

21 *Id*. at Section 7.D(3)(g).

22 Conn. S.B. 949 (2015), Public Act 15-142.

23 Cal. Civ. Code §1798.82.

24 Please see "Remarks of Acting OPM Director Beth Cobert," *available at* https://www.opm.gov/news/speeches-remarks/carrier-conference/.

Practical Pointers

Unlike the financial and health care sectors, whose cybersecurity preparedness has been scrutinized by federal regulators for a number of years, insurers may have been able to avoid this intense focus until more recently. As a result, many insurance companies may be leanly staffed in cybersecurity and perhaps less mature than their counterparts in banking and health care.

Going forward, insurers need to keep a close watch on how the NAIC model law develops and whether it is enacted in a state where they do business. In addition, companies can take action now by updating their incident response plans to implement the more noteworthy provisions of the law, such as the short notice period and requirement to provide credit monitoring or other identity theft protection.

Finally, in the current cyber threat environment, resources spent shoring up cyber defenses and preparedness will most certainly be wisely spent.

If you would like to receive future *Privacy & Data Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Marianne Roach Casserly
202.239.3379
marianne.casserly@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Jon Filipek
+32 2 550 3754
jon.filipek@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

Katherine E. Hertel
213.576.2600
kate.hertel@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Dominique R. Shelton
213.576.1170
dominique.shelton@alston.com

Paula M. Stannard
202.239.3626
paula.stannard@alston.com

David M. Stein
213.576.1063
david.stein@alston.com

Brian Stimson
404.881.4972
brian.stimson@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Jeffrey E. Tsai
650.838.2095
213.576.2608
jeff.tsai@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Michael Zweiback
213.576.1186
michael.zweiback@alston.com

ALSTON&BIRD

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com