Report of the

Multistate Targeted Market Conduct and Financial Examination

for the

California Department of Insurance

Indiana Department of Insurance

Maine Bureau of Insurance

Missouri Department of Insurance

New Hampshire Insurance Department

North Dakota Insurance Department

South Carolina Department of Insurance

and

Other Participating Jurisdictions:

Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming, American Samoa, Guam, Puerto Rico, the United States Virgin Islands, and the Northern Marianas Islands

of

Anthem Insurance Companies, Inc. and its Affiliates

120 Monument Circle
Indianapolis, Indiana
NAIC Group # 0671

December 1, 2016

Contents

December 1, 2016

The Honorable Stephen W. Robertson
Commissioner
Indiana Department of Insurance
311 West Washington Street, Suite 103
Indianapolis, Indiana 46204-2787

The Honorable Adam Hamm
Commissioner
North Dakota Insurance Department
600 East Boulevard Avenue, 5th Floor
Bismarck, North Dakota 58505-0320

The Honorable Dave Jones
Commissioner
California Department of Insurance
300 Capitol Mall, 17th Floor
Sacramento, California 95814

The Honorable Roger A. Sevigny
Commissioner
New Hampshire Insurance Department
21 Fruit Street, Suite 14
Concord, New Hampshire 03301

The Honorable Raymond G. Farmer
Director
South Carolina Department of Insurance
P.O. Box 100105
Columbia, South Carolina 29202-3105

The Honorable John M. Huff
Director
Missouri Department of Insurance
Financial Institutions and Professional Registration
P.O. Box 690
Jefferson City, Missouri 65102-0690

The Honorable Eric A. Cioppa
Superintendent
Department of Professional and Financial Regulation
Maine Bureau of Insurance
34 State House Station
Augusta, Maine 04333-0034

Dear Commissioners Robertson, Hamm, Jones, and Sevigny; Directors Farmer and Huff; and Superintendent Cioppa:

Pursuant to a February 26, 2015 Examination Warrant issued by the Indiana Department of Insurance and the authority granted by CAL. INS. CODE § 730, INDIANA CODE § 27-1-3.1-8, ME. REV. STAT. § 221, MO. REV. STAT. § 374.205, N.H. REV. STAT. ANN. § 400-A:37 N.D. CENT. CODE § 26.1-03-19.2, AND S.C. CODE ANN. § 38-13-10, (the "Examination Statutes"), a targeted multistate market conduct and financial examination was noticed regarding a data breach publicly announced on February 5, 2015 respecting:

Anthem Insurance Companies, Inc.
and its affiliated companies
(collectively "Anthem" or the "Company")

The examination was conducted in accordance with the National Association of Insurance Commissioners *Market Regulation Handbook and Financial Condition Examiners Handbook* ("*Handbooks*"), to the extent applicable. The report of examination is herewith respectfully submitted.

Alvarez & Marsal Insurance and Risk Advisory Services, LLC

Examiners-In-Charge

Foreword

This report on the multistate targeted examination of the Company is provided pursuant to the *Handbooks*. The principal examination work was conducted by Alvarez & Marsal Insurance and Risk Advisory Services, LLC; Alvarez & Marsal Global Forensic and Dispute Services; and CrowdStrike Services, Inc. ("CrowdStrike") (collectively, the "Examination Team").

On February 4, 2015, Anthem notified the Indiana Department of Insurance, its principal domiciliary regulator, that it was investigating a potentially serious data security breach first discovered on January 27, 2015 ("Data Breach"). Anthem also informed regulators that it had retained Mandiant, a cybersecurity consulting firm, to assist the Company with its internal investigation of the incident. The Indiana Department of Insurance then notified the National Association of Insurance Commissioners ("NAIC") Market Analysis Working Group. Anthem publicly announced the Data Breach on February 5, 2015. On February 26, 2015, the Indiana Department of Insurance advised the Company that a targeted examination had been called to assess Anthem's state of cybersecurity preparedness prior to the Data Breach, its post-breach response, and the adequacy of measures taken by Anthem to mitigate harm to consumers ("Examination"). Additionally, the Examination Team was asked to determine the identity of the actors responsible for this breach. The Examination was conducted on a multistate basis with Indiana as the Coordinating Lead State, California, New Hampshire, North Dakota, Maine, South Carolina and Missouri as Co-Lead States, and all other members of the NAIC joining as participating jurisdictions.

Profile of the Companies

Anthem is the nation's largest health benefits company by membership, with member insurers licensed to conduct business in all fifty states and the District of Columbia. The

Company is headquartered in Indianapolis, Indiana, and markets products and services in multiple jurisdictions either using its own name or the name and marks of Blue Cross Blue Shield or affiliates such as UniCare, CareMore, and Amerigroup. The parent company is a publicly traded company.

Examination Purpose, Scope, and Structure

The purpose of the Examination was to assess Anthem's state of cybersecurity preparedness prior to the Data Breach, assess its post-breach response, assess the adequacy of measures taken by Anthem to mitigate harm to consumers, and determine the identity of the actor(s) responsible for the breach (the "Attacker"). The Examination's scope included all U.S. jurisdictions and included the period from February 18, 2014, the date the Data Breach began, through July 15, 2015, the last date on which Anthem provided information to the Examination Team. The Examination was conducted under the authority of the Examination Statutes.

The Examination Team did not conduct an independent investigation of the Data Breach. Instead, the Lead States directed that the Examination Team review the suitability of Anthem's systems and security protocols prior to the breach, its reaction to the Data Breach, and subsequent efforts to address system security and remediate consumer impacts. The Examination therefore included both elements of independent examination and peer review regarding the work performed by Anthem and its retained cybersecurity vendor, Mandiant.

The Examination Team's work included four principal phases: (i) Integration; (ii) Initial Assessment; (iii) Breach Assessment; and (iv) Cybersecurity Assessment. The key elements of each phase included:

Integration

- Meet with key Anthem personnel, representatives of the Lead States, and the Examination Team
- Provide an initial data request to Anthem

- Develop protocols for communication, information flow, documentation, and reporting

Initial Assessment

- Interview key Anthem and Mandiant personnel to orient the Examination Team to the Data Breach and Anthem's response
- Obtain technical documents and materials associated with Anthem's pre-breach cybersecurity environment, its response to the Data Breach, and the efforts that took place post-breach to assess vulnerabilities in Anthem's cybersecurity program

Breach Assessment

- Review Anthem's technical scoping of the Data Breach, the analysis that was conducted, and the technical and business conclusions reached
- Review the actions taken by Anthem and Mandiant to detect, contain and respond to the Data Breach, including consumer protections

Cybersecurity Assessment

- Conduct an in-depth review of the cybersecurity controls that were in place prior to the Data Breach and the controls that are currently in place
- Perform an external limited-in-scope penetration test to determine whether Anthem's controls appeared to be effective to detect and/or prevent another breach using tactics, techniques, and procedures similar to those used by the Attacker perpetrating the Data Breach

The Examination Team began work in May of 2015, and submitted a draft confidential report on July 20, 2015 (the "Confidential Report"). The Examination Team discussed its findings and conclusions with the Lead States.

Examination Findings

This examination report is intended for public distribution and, accordingly, does not reflect all findings, analysis and information contained in the Confidential Report as the Confidential Report contains confidential and proprietary information. This examination report summarizes the points necessary to understand what occurred and to answer the regulatory questions giving rise to the Examination Purpose. This examination report is subject in all

respects to the limiting conditions described in the attached appendix entitled "Limitations of Report." The examination findings are presented below in six sections: The Data Breach, Pre-Breach Cybersecurity, Pre-Breach Response Preparation, Response Adequacy, Post-Breach Cybersecurity, and Corrective Actions.

The Data Breach – Anthem discovered the Data Breach on January 27, 2015, and immediately informed the Federal Bureau of Investigation that it was investigating a potentially serious security breach. Anthem also engaged Mandiant to assist the Company with its post-breach response. The Company implemented its Incident Response Plan ("IR Plan"), and the last successful malicious activity was noted by Anthem on January 30, 2015. Subsequent investigation by the Company and Mandiant determined that the Data Breach began on February 18, 2014, when a user in Anthem's Amerigroup subsidiary opened an e-mail (commonly referred to as a "phishing" e-mail) containing malicious content. Opening this e-mail permitted the download of malicious files to the user's local system, allowing the Attacker to gain remote access to that computer.

Starting with the initial remote access, the Attacker was able to move laterally (across Anthem systems) and escalate privileges (gain increasingly greater ability to access information and make changes in Anthem's environment). The Attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the Company's enterprise data warehouse – a system that stores a large amount of consumer personally identifiable information ("PII"). Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 million unique user records.

Examination Team members from CrowdStrike determined the identity of the Attacker with high confidence.[1] CrowdStrike also concluded with medium confidence that the Attacker was acting on behalf of a foreign government. In CrowdStrike's experience, attacks associated with this foreign government have not resulted in PII being transferred to non-state actors.

Pre-Breach Cybersecurity – The Examination Team evaluated whether Anthem had in place, prior to the Data Breach, a cybersecurity program suitable for a company of its size, operations, and business purpose. In our view, Anthem appeared to have taken reasonable measures prior to the Data Breach to protect its computer network and data. Those measures included the implementation of cybersecurity technologies and procedures consistent with or exceeding those of a typical organization of its size and type. However, the Attacker was able to exploit certain cybersecurity gaps which allowed the Data Breach to occur.

Pre-Breach Response Preparation - Our review disclosed that prior to the breach the Company had a detailed IR Plan in place. The IR Plan documented roles, responsibilities, and processes related to incident response, and those procedures had been tested in several "tabletop" exercises prior to the Data Breach.

Response Adequacy – The Examination Team investigated whether Anthem's execution of the IR Plan resulted in a rapid and effective response to the Data Breach. Our review determined that, once the breach was detected, Anthem's cybersecurity personnel immediately involved top management, took immediate investigative action to ascertain the magnitude of the breach, and took remediation steps to contain the breach. The Company also communicated with

[1] For purposes of attacker attribution, CrowdStrike's confidence assessments were based on: **High** - Information on the subject is of high quality from multiple sources or from a single highly reliable source, and the nature of the issue makes it possible to render a solid judgment; **Medium** - Information on the subject is interpreted various ways, alternating views exist, or the information, while credible, is of insufficient reliability to warrant a higher level of confidence; and **Low** - Information on the subject is scant, questionable, or very fragmented; it is difficult to make solid analytic inferences; or significant concerns or problems with the source exist.

law enforcement officials, regulators, and the public in a timely manner. Anthem's response to the Data Breach therefore appeared to be timely and effective, and removed the Attacker's ability to access the network within three days of identifying the Data Breach.

Post-Breach Cybersecurity – Following the Data Breach, Anthem engaged Mandiant to investigate the Data Breach, assess the adequacy of its cybersecurity controls, and recommend steps to improve its security posture. Anthem advised the Examination Team that it had implemented two-factor authentication on all remote access tools, deployed a "Privileged Account Management" solution, and added enhanced additional logging resources to its existing security event and incident management solutions. Further, the Company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication, and created new Network Admin IDs to replace existing IDs. Going forward, Anthem acquired additional technology to improve its monitoring capabilities in critical databases.

The Examination Team noted exploitable vulnerabilities in the immediate aftermath of the Data Breach, and that Anthem had developed a remediation plan to address those issues. It is the Examination Team's view that Anthem's improvements to its cybersecurity protocols and schedule of planned future improvements appeared to be reasonable efforts to secure the environment beyond the initial Data Breach remediation tasks.

Corrective Actions – After discovering the Data Breach, Anthem promptly communicated and cooperated with law enforcement and regulatory officials. The Company also notified the public and affected individuals through direct mail, e-mail, news publications, website notice, and working with state insurance departments. Within two weeks of discovering the Data Breach, the Company also engaged a consumer credit protection company to provide

credit protection services to all breach-affected consumers. Anthem provided credit protection services for a two-year period. Anthem's consumer protections were at least equal to those afforded to consumers in the other breach situations with which the Examination Team was familiar.

Summary

The Attacker exploited weaknesses in Anthem's information security processes and technology to access and exfiltrate a large quantity of Anthem customer data. Once the Data Breach was identified, Anthem responded quickly and effectively to the Attacker's presence in its network, fully removing the Attacker's access to the network within three days. While deficiencies within Anthem's cybersecurity posture were noted by the Examination Team, these deficiencies were not, in our experience, uncommon to companies comparable to Anthem in size and scope. While the pre-breach deficiencies impacted Anthem's ability to reduce the likelihood of and quickly detect the Data Breach, the controls implemented subsequent to the Data Breach should improve Anthem's ability to detect future breaches and enable Anthem to respond more effectively to a future attack than was the case in this instance.

Verification and Report Submission

The foregoing is a true and accurate report of the Examination. The report of examination in herewith respectfully submitted.

Sincerely,

Neil A. Miller
Examiner-in-Charge
Alvarez & Marsal Insurance and Risk Advisory Services, LLC

Acknowledgement

The Examination Team extends our sincere thanks and appreciation to Commissioner Robertson and his staff at the Indiana Department of Insurance for their leadership and facilitation of this examination. We also wish to thank the other Lead States for their leadership and assistance on this examination.

The Examination Team further acknowledges and thanks Anthem for all of their work in facilitating this examination, and for the courtesies they extended to us throughout this examination.

Appendix - Limitations of Report

This report and the information contained herein ("Information") has been prepared solely for use by the Indiana Department of Insurance ("IDOI"), other Lead States and participating jurisdictions (the "Intended Recipients").

The Examination Team assumes no duties or obligations to any recipient of this report by virtue of their access hereto save as set forth in a separate written agreement between the Examination Team and such recipient. The limiting conditions and disclaimers set forth herein are an integral part of this report, must be reviewed in conjunction herewith, and may not be modified or distributed separately. Any use or potential publication of this report is not intended nor should it be construed as a waiver of any privilege or immunity from disclosure that may attach to the Examination Team's privileged work, investigation, and reports.

This report has been prepared and compiled as a summary of the Examination Team's efforts to assist the IDOI in evaluating issues related to the cybersecurity breach of Anthem and does not purport to contain all necessary information that may be required to evaluate the Data Breach and response, regardless of how pertinent or material such information may be. The scope of the examination did not include verification of any of the underlying source data which provides a basis for the descriptions and findings in the report. Accordingly, the Examination Team makes no representation or warranty as to the accuracy, reliability or completeness of the information. No member of the Examination Team is responsible to any party, in any way, for any representation, analysis, or findings contained in the report, or the manner in which the report may be used.

This report and any related advice or Information is provided solely for the use and benefit of the Intended Recipients and only in connection with the purpose in respect of which

the services are provided. In no event, regardless of whether consent has been provided, shall the Examination Team assume any responsibility, liability or duty of care to any person or entity other than the IDOI and Lead States. This report does not take account of those matters or issues which might be of relevance to any entity or person. The Examination Team has not considered any such matters or issues, and any third party is responsible for conducting its own investigation with respect to the Information and any related transactions or activities. The Examination Team makes no representations or warranties, express or implied, to any third party on which any such party may rely with respect to the Information, including without limitation, as to accuracy or completeness, the inclusion or omission of any facts or information, or as to its suitability, sufficiency or appropriateness for the purposes of any such party.

This report serves as a point-in-time assessment of the Anthem environment. Any and all security controls or processes that are implemented after the examination was completed are considered outside the scope of the assessment.