XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
YEN P. NGUYEN (SBN 239095)
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102
Telephone: (415) 510-3497
Fax: (415) 703-1234
E-mail: TiTi.Nguyen@doj.ca.gov

Attorneys for The People of the State of California

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA

UNLIMITED JURISDICTION

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, v. **ANTHEM, INC.**, a corporation, Defendant.	Case No. RG20075118 **[PROPOSED] FINAL JUDGMENT AND PERMANENT INJUNCTION** (Cal. Bus. & Prof. Code, § 17200 *et seq.*)

Plaintiff, the People of the State of California ("the People" or "Plaintiff"), appearing through its attorney, Xavier Becerra, Attorney General of the State of California, by Yen P. Nguyen, Deputy Attorney General, and Stacey D. Schesser, Supervising Deputy Attorney General, and Defendant Anthem, Inc. ("Anthem"), a corporation, appearing through its attorneys Craig Hoover, Michelle Kisloff, Allison Holt Ryan, Adam Cooke, and Vassi Iliadis of Hogan Lovells US LLP, having stipulated to the entry of this Final Judgment and Permanent Injunction ("Judgment") by the Court with all parties having waived their right to appeal, and the Court having considered the matter and good cause appearing:

IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. INTRODUCTION

This Judgment arises from a data breach, publicly announced by Anthem on February 4, 2015, in which a criminal cyber-attacker gained unauthorized access to its network and infiltrated an internally-hosted enterprise data warehouse, which contained the personal information ("PI") and/or protected health information ("PHI") of Anthem plan members and other individuals (the "Data Breach"). Anthem discovered the unauthorized access that caused the Data Breach on or about January 29, 2015. The Data Breach affected approximately 78,800,000 individuals nationwide. The information accessed in unencrypted form by the cyber-attacker included names, dates of birth, Social Security numbers, healthcare identification numbers, home addresses, email addresses, phone numbers, and employment information, including income data.

II. PARTIES AND JURISDICTION

1. For purposes of this action, this Court has jurisdiction over the allegations and subject matter of the People's Complaint and the parties to this action; venue is proper in this County; and this Court has jurisdiction to enter this Judgment.

III. DEFINITIONS

2. For the purposes of this Judgment, the following definitions shall apply:

a. "Anthem" shall mean Anthem, Inc., its wholly owned, integrated, and operated affiliates, subsidiaries, and divisions, successors, and assigns, directors and officers and employees doing business in the United States.

b. "Anthem Network" shall mean the networking equipment, databases or data stores, applications, servers, and endpoints that are capable of using and sharing software, data, and hardware resources and that are owned and/or operated by Anthem.

c. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to PHI.

d. "Consumer Protection Act" shall mean Business & Professions Code section 17200 *et seq.*

e. "Covered Entity" shall be defined in accordance with 45 C.F.R. § 160.103 as a health plan, health care clearinghouse, or health care provider that transmits protected health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted standards.

f. "Covered Systems" shall mean components, such as servers, workstations, and devices, within the Anthem Network that are routinely used to collect, process, communicate, and/or store PI and/or PHI.

g. "Data Breach" shall mean the security incident discovered by Anthem on or about January 29, 2015, and publicly announced on February 4, 2015, in which a malicious cyber-attacker gained unauthorized access to portions of the Anthem Network that stored PI and/or PHI, and which impacted approximately 78,800,000 individuals nationwide.

h. "Data Breach Notification Law" shall mean Civil Code section 1798.82.

i. "Effective Date" shall be October 30, 2020.

j. "Encrypt," "Encrypted," or "Encryption" shall refer to the transformation of data at rest or in transit into a form in which meaning cannot be assigned without the use of a confidential process or key. The manner of Encryption shall conform to existing industry standard.[1]

k. "Minimum Necessary Standard" shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).

[1] For the purposes of this Judgment, the term "existing industry standard" applies to what the standard may become as the industry changes over time. As of the Effective Date, the existing industry standard shall be defined pursuant to Federal Information Processing Standards Publication 140-2.

l. "Multi-factor Authentication" means authentication through verification of at least two of the following authentication factors: (i) knowledge factors, such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.

m. "Personal Information" or "PI" shall mean the data elements in the definition of personal information set forth in the Data Breach Notification Law and/or Personal Information Protection Act.

n. "Personal Information Protection Act" shall mean Civil Code section 1798.85.1.

o. "Privacy Rule" shall refer to the HIPAA Regulations that establish national standards for safeguarding individuals' medical records and other Protected Health Information, including electronic PHI, that is created, received, used, or maintained by a Covered Entity or a Business Associate, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

p. "Protected Health Information" or "PHI" shall be defined in accordance with 45 C.F.R. § 160.103, including electronic protected health information.

q. "Security Event" shall mean any compromise that (i) results in the unauthorized access, acquisition, or exfiltration of electronic PI or PHI collected, processed, transmitted, stored, or disposed of by Anthem, or (ii) causes lack of enterprise availability of electronic PI or PHI of at least 500 U.S. consumers held, processed, or stored by Anthem.

r. "Security Rule" shall refer to the HIPAA Regulations that establish national standards to safeguard individuals' electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

IV. INJUNCTIVE PROVISIONS

The injunctive terms contained in this Judgment are being entered pursuant to Business and Professions Code section 17203.

A. Compliance with State Law

3. Anthem shall not misrepresent the extent to which Anthem maintains and protects the privacy, security, or confidentiality of any PI or PHI collected from or about consumers.

4. If a Security Event does not trigger the Data Breach Notification Law, Anthem shall create a report that includes a description of the Security Event and Anthem's response to that Security Event ("Security Event Report"). The Security Event Report shall be made available for inspection by the Third-Party Security Assessor as described in Paragraph 28.

B. Information Security Program

5. Anthem shall develop, implement, and maintain a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI that Anthem collects, stores, transmits, maintains, and/or destroys. The Information Security Program, shall, at a minimum, include the specific information security requirements set forth in Paragraphs 6 through 26 of this Judgment.

a. The Information Security Program shall comply with any applicable requirements under state or federal law, and shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Anthem's operations; (ii) the nature and scope of Anthem's activities; and (iii) the sensitivity of the PI and PHI that Anthem collects, stores, transmits and/or maintains.

b. The Information Security Program shall be written and modified to allow access to PHI consistent with the Minimum Necessary Standard. Anthem shall consider and adopt where reasonably feasible the principles of zero trust architecture throughout the Anthem Network. As used herein, zero trust architecture means Anthem will:

i. Regularly monitor, log, and inspect network traffic, including log-in attempts, through the implementation of hardware, software, or procedural mechanisms that record and evaluate such activity;

ii. Authorize and authenticate relevant device, user, and network activity within the Anthem Network; and

iii. Require appropriate authorization and authentication prior to any user's access to the Anthem Network.

c. Anthem may satisfy the requirements of this Judgment, including the implementation of the Information Security Program, through the review, maintenance, and, if necessary, updating of an existing information security program or existing safeguards, provided that such existing program or safeguards meet the requirements set forth in this Judgment.

d. Anthem shall review not less than annually the Information Security Program.

e. Anthem shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program ("Chief Information Security Officer" or "CISO"). The CISO shall have the background and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program.

f. The role of the CISO will include regular and direct reporting to the Chief Executive Officer ("CEO"), Executive Staff, and Board of Directors concerning Anthem's security posture, the security risks faced by Anthem, and the security implications of Anthem's business decisions. The CISO shall meet with and provide a report to: (1) the Board of Directors on at least a semi-annual basis and (2) the CEO on at least a quarterly basis. The CISO shall report to the CEO within twenty-four (24) hours of a confirmed Security Event impacting 500 or more consumers residing in the United States. The CISO shall include such Security Events in its annual report to the Board of Directors.

g. Anthem shall provide notice of the requirements of this Judgment to the employees of Anthem's Information Security organization and shall implement training on the requirements of this Judgment to those employees. Anthem shall provide the training required under this Paragraph to such employees within ninety (90) days of the Effective Date of this Judgment or prior to their starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

h. As part of its Information Security Program, Anthem shall develop, implement, and maintain a written incident response plan to prepare for and respond to Security Events. Anthem shall revise and update this response plan, as necessary, to adapt to any material changes that affect the security of PI and PHI. Such a plan shall, at a minimum, identify and describe the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Eradication; (vi) Recovery; (vii) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis.

i. Anthem shall budget such that its Information Security Program receives the resources and support reasonably necessary to function as intended.

j. Anthem shall take reasonable efforts, using a reasonable and documented risk-based approach, to evaluate whether vendors that routinely handle PI or PHI have safeguards in place to protect such information and that such vendors will notify Anthem promptly of any potential compromise to the confidentiality, integrity, or availability of PI or PHI held, stored, or processed by the vendors on behalf of Anthem.

C. Specific Information Security Requirements

6. **Data Collection & Retention**: Anthem shall develop, implement, and maintain reasonable policies and procedures governing its collection, use, and retention of PI and PHI. Anthem shall limit its use, disclosure of, and requests for PHI in accordance with the Minimum Necessary Standard, and to fulfill all applicable regulatory, legal, and contractual obligations.

7. **Segmentation**: Anthem shall develop, implement, and maintain reasonable policies and procedures designed to reasonably segment the Anthem Network. At a minimum, within ninety (90) days, Anthem shall develop a timetable to implement:

a. segmentation of its VOIP servers; and

b. segmentation of its development and production environments.

On a semiannual basis, Anthem will report to the Board of Directors regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

8. **Cyber Security Operations Center ("C-SOC")**: Anthem shall maintain the existence and operation of its C-SOC or a reasonably equivalent technology. The C-SOC shall be staffed continuously to provide comprehensive monitoring of servers and other technologies to identify improper use of data, including PI and/or PHI. The C-SOC's analytic capabilities shall be deployed to detect, analyze, and respond to potential and confirmed Security Events.

9. **Logging & Monitoring**: Anthem shall develop, implement, and maintain reasonable policies and procedures designed to properly log and monitor the Anthem Network. At a minimum:

a. Anthem shall employ tools, such as a Security Information and Event Monitoring solution ("SIEM") (or a reasonably equivalent technology), among others, to log and monitor network traffic to detect and respond to Security Events.

b. Anthem shall take reasonable steps to properly configure, and regularly update or maintain the SIEM (or a reasonably equivalent technology) used pursuant to subsection (a) and shall take reasonable steps to adequately log system activity and identify potential Security Events for review. Using the SIEM (or a reasonably equivalent technology), Anthem shall actively review and analyze in real-time the logs of system activity and take appropriate follow-up with respect to Security Events.

c. Anthem shall maintain logs in conformance with industry standards and all applicable laws.

d. In addition to the requirements set forth in subparagraphs (a) through (c) of this Paragraph, Anthem shall develop, implement, and maintain defined and specific policies and procedures with respect to logging and monitoring of the internal data warehouse involved in the Data Breach and any database (or set of databases) that collects, processes, transmits, and/or stores PI and/or PHI of similar volume as the internal data warehouse involved in the Data Breach. At a minimum:

i. Anthem shall deploy an appropriate database activity monitoring tool or a reasonably equivalent technology in the internal data warehouse involved in the Data Breach and any similar database (or set of databases) that Anthem uses to collect, process,

transmit, and/or store PI and/or PHI of similar volume as the internal data warehouse involved in the Data Breach, to the extent it is commercially feasible.

ii. The monitoring of such database(s) shall include commercially reasonable query categories available in a database activity monitoring tool or reasonable equivalent issued to the relevant database(s).

iii. The monitoring of such database(s) shall be performed by appropriately trained or experienced personnel.

e. Anthem shall create a formalized procedure to track Security Events and alerts on privileged user queries on a regular basis and document identified issues and necessary action items.

10. **Antivirus Maintenance**: Anthem shall implement and maintain current, up-to-date antivirus protection programs or a reasonably equivalent technology on the Anthem Network components that require antivirus software, which shall be at the highest technical level available within Anthem-approved antivirus products that can be supported on such components, subject to any reasonable and documented security exceptions.

11. **Access Controls**: Anthem shall implement and maintain appropriate controls to manage access to and use of all accounts with access to PI or PHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Such controls shall include a means to regularly review access and access levels of users and remove network and remote access within twenty-four (24) hours of notification of termination for any employee whose employment has ended or any non-associate whose term has ended.

12. **Authentication**: Anthem shall implement and maintain reasonable policies and procedures requiring the use of authentication in accordance with industry standards, where commercially feasible, including as appropriate under industry standards, the use of strong passwords, password rotation, and ensuring that stored passwords are protected from unauthorized access.

13. **Privileged Account Management**: Anthem shall implement and maintain reasonable controls to secure use of privileged credentials, such as through a Privileged Access

Management tool or reasonably equivalent technology that vaults and rotates elevated credentials in places where privileged access credentials are required. Administrators shall be required to use Multi-factor Authentication or reasonably equivalent technology to gain access to their safe within the vault to retrieve their credentials.

14. **Remote Access / Multi-factor Authentication**: Anthem shall require the use of Multi-factor Authentication or reasonably equivalent technology for end-user remote access to the Anthem Network that are servers. Additionally, Anthem will require during vendor security assessments business record documentation that demonstrates the vendor deploys Multi-factor Authentication or reasonably equivalent technology for end-user remote access to the Anthem Network via any business-to-business connection.

15. **Encryption**: Anthem shall develop, implement, maintain, regularly review, and revise policies and procedures to Encrypt PI and PHI at rest and in transit as reasonable and appropriate, and in accordance with applicable law.

16. **Asset Inventory**: Anthem shall develop, maintain, and regularly update a reasonable inventory of the assets that primarily comprise the Anthem Network and assign criticality ratings to such assets, as feasible.

17. **Risk Assessments**: Anthem shall develop, implement, and maintain a risk assessment program to identify, address, and, as appropriate, remediate risks affecting its Covered Systems. At a minimum, Anthem shall have an annual risk assessment performed by an independent third party. The assessment shall include assessment of all reasonably anticipated, internal and external risks to the security, confidentiality, or availability of PI and PHI collected, processed, transmitted, stored, or disposed of by Anthem, excluding legal documents and analyses that Anthem reasonably asserts are exempt from disclosure under legally-recognized privilege. Such reports shall be maintained by the CISO and be made available for inspection by the Third-Party Assessor described in Paragraph 28 of this Judgment.

18. **Vulnerability Management**: Anthem shall commit to continuing its current practices related to vulnerability scanning or a reasonably equivalent technology and remediation.

19. **Penetration Testing**: Anthem shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within the Anthem Network, which shall include annual external penetration tests or a reasonably equivalent technology and appropriate remediation of vulnerabilities revealed by such testing. Anthem shall develop, implement, and maintain an internal penetration testing program through the use of its Adversary Simulation Team or a reasonably equivalent group, who shall perform biannual internal penetration tests. The reports of such external and internal penetration tests shall be maintained by the CISO for a period of not less than six (6) years and be made available for inspection by the Third-Party Assessor described in Paragraph 28 of this Judgment.

20. **Email Filtering and Phishing Solutions**: Anthem shall maintain email protection and filtering solutions for all Anthem email accounts, including email SPAM, phishing attacks, and anti-malware or a reasonably equivalent technology.

21. **Employee Training**: In addition to the requirements set forth in Paragraph 5(g) above, Anthem shall conduct an initial training for all new employees and, on at least an annual basis, train existing employees concerning its information privacy and security policies, the proper handling and protection of PI and PHI, and disciplinary measures for violation, up to and including termination. At a minimum:

a. Anthem's new employee and annual training shall cover social engineering schemes, such as phishing;

b. Anthem shall conduct annual mock phishing exercises and all employees who fail must successfully complete additional training; and

c. Anthem shall document such trainings and the results of the mock phishing exercises.

22. **Network Sensors**: Anthem shall deploy network sensors or a reasonably equivalent technology to detect attempts to communicate from the Anthem Network to known malicious IP addresses.

23. **Endpoint Detection and Response**: Anthem will implement, maintain, and monitor controls designed to provide real-time notification of malicious systems modifications and anomalous systems activity in the Covered Systems.

24. **Intrusion Detection and Prevention Solution(s)**: Anthem shall develop, implement, and maintain an intrusion detection and prevention solution to assist in detecting and preventing unauthorized access to the Anthem Network.

25. **Data Loss Prevention**: Anthem shall develop, implement, and maintain a data loss prevention technology or a reasonably equivalent technology to detect and prevent unauthorized data exfiltration from the Anthem Network.

26. **Whitelisting**: Anthem shall implement and maintain controls designed to identify applications permitted to be on the Covered Systems while blocking and/or preventing the execution of unauthorized applications (*i.e.*, applications not on the whitelist) on critical servers.

D. Information Security Program Assessment

27. Anthem shall obtain an initial and annual information security assessment of its policies and practices pertaining to the collection, storage, maintenance, transmission, and disposal of PI and PHI, from an independent third-party professional ("Third-Party Assessor") within one year of the Effective Date of this Judgment and then once a year thereafter for a total period of three (3) years.

28. The Third-Party Assessor must be an organization that employs at least one individual to perform the assessment that is: (a) qualified as a Certified Information System Security Professional ("CISSP") or as a Certified Information Systems Auditor ("CISA"), or a similar qualification; and (b) has at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

29. Anthem may satisfy the initial assessment by providing a copy of the Assessment Report performed for calendar year 2019 pursuant to the settlement of *In re Anthem Inc. Data Breach Litig.*, MDL 2617. For the remaining two assessments, the Third-Party Assessor shall review this Judgment or the Assurance of Voluntary Compliance ("Assurance") between Anthem and the Connecticut Attorney General with the same Effective Date as this Judgment, as well as

the Security Event Report, risk assessments, and penetration test reports provided by Anthem as set forth in Paragraphs 4, 17, and 19, respectively. The Third-Party Assessor shall prepare a formal report ("Security Report") that shall confirm Anthem's development, implementation, and maintenance of a written Information Security Program with security controls and processes that meet the requirements of this Judgment or the Assurance related to: segmentation, antivirus maintenance, access controls including privileged access management and multi-factor authentication, vulnerability scanning and remediation, logging and monitoring, encryption, application whitelisting, e-mail filtering, and information system activity review and detection. The Security Report shall also confirm that Anthem has complied with the provisions of this Judgment or the Assurance related to the employment of a CISO or equivalent officer, maintenance of a C-SOC facility, and performance of internal and external penetration tests and information security training. In preparing each Security Report, the Third-Party Assessor may rely on the Assessment Report performed for calendar years 2020 and 2021 for *In re Anthem Inc. Data Breach Litig.*, MDL 2617, for security controls and processes addressed by both that Assessment Report and this Judgment or the Assurance.

30. The Security Report shall be provided to the Attorney General no later than ten (10) days after its completion. Anthem will also provide the Risk Assessment, as set forth in Paragraph 17, and a SOC 2 Type 2 Assessment, as referenced in Paragraph 32 to the Attorney General on an annual basis during the three-year term.

a. Confidentiality: The Attorney General's Office shall, to the extent permitted by state law, treat each Security Report, Risk Assessment, and SOC 2 Type 2 Assessment as exempt from disclosure as applicable under the relevant public records laws.

31. Upon receipt of each Security Report, Anthem will review and evaluate whether to revise its current policies and procedures based on the findings of the Security Report. Within sixty (60) days of Anthem's receipt of each Security Report, Anthem shall forward to the Attorney General a description of any action they plan to take, or if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

E. Information Security Program Audit

32. Anthem shall provide to the Attorney General an annual SOC 2 Type 2 Assessment for calendar year 2019 and then once a year thereafter for a total period of three (3) years. At a minimum, this Assessment shall include the trust service principles of Security and Confidentiality.

V. PAYMENT TO THE STATE

33. Pursuant to Business and Professions Code section 17206, Anthem shall pay the Attorney General the amount of $8,690,000.00, which shall be allocated and used in accordance with Business and Professions Code section 17206. Payment shall be made by wire transfer to the Attorney General's Office pursuant to instructions provided by the Attorney General's Office.

VI. RELEASE AND EXPIRATION

34. Release: Following full payment of the amounts due by Anthem under this Judgment, the Attorney General shall release and discharge Anthem from all civil claims that the Attorney General could have brought under the Consumer Protection Act, Personal Information Protection Act, Security Breach Notification Act, and Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1938, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, and any common law claims concerning unfair, deceptive, or fraudulent trade practices based on Anthem's conduct related to the Data Breach. Nothing contained in this paragraph shall be construed to limit the ability of the Attorney General to enforce the obligations that Anthem, its officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns, have under this Judgment. Further, nothing in the Judgment shall be construed to create, waive, or limit any private right of action.

35. Notwithstanding any term of this Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 34 as to any entity or person, including Anthem:

a. Any criminal liability that any person or entity, including Anthem, has or may have to the State of California.

b. Any civil or administrative liability that any person or entity, including Anthem, has or may have to the State of California under any statute, regulation or rule giving rise to, any and all of the following claims:

i. State or federal antitrust violations;

ii. State or federal securities violations; or

iii. State or federal tax claims.

36. Expiration: The obligations and other provisions of this Judgment set forth in Paragraphs 5.b, 7-14, 16, 18-20, and 22-26 shall expire at the conclusion of the five (5) year period after the Effective Date of this Judgment. The obligations and other provisions of this Judgment set forth in Paragraphs 15, 17, 21(a)-(c), 46, and 47 shall expire at the conclusion of the seven (7) year period after the Effective Date of the Judgment, unless they have expired at an earlier date pursuant to their specific terms. Provided, however, that nothing in this Paragraph shall be construed as excusing or exempting Anthem from complying with any state or federal law, rule, or regulation, nor shall any of the provisions of this Judgment be deemed to authorize or require Anthem to engage in any acts or practices prohibited by any law, rule, or regulation.

VII. GENERAL PROVISIONS

37. Meet and Confer. If the Attorney General determines that Anthem has failed to comply with any of the terms of this Judgment, and if in the Attorney General's sole discretion the failure to comply does not threaten the health or safety of the State of California and/or does not create an emergency requiring immediate action, the Attorney General will notify Anthem in writing of such failure to comply and Anthem shall have thirty (30) days from receipt of such written notice to provide a good faith response to the Attorney General's determination. The response shall include: (A) a statement explaining why Anthem believes it is in full compliance with this Judgment; or (B) a detailed explanation of how the alleged violation(s) occurred, and either (i) a statement regarding whether the alleged violation(s) has been addressed and how, or (ii) a statement regarding whether the alleged violation cannot be reasonably addressed within thirty (30) days receipt of the notice, but, if (B)(ii) then also a statement (a) indicating whether Anthem has begun to take corrective action(s) to address the alleged violation(s), (b) stating what

corrective action(s) Anthem is pursuing, and (c) providing the Attorney General with a reasonable timetable for addressing the alleged violation(s). Nothing herein shall prevent the Attorney General from agreeing in writing to provide Anthem with additional time beyond the thirty (30) day period to respond to the notice referenced in this Paragraph. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Judgment after the Effective Date or compromise the authority of the Attorney General to initiate a proceeding for any failure to comply with this Judgment.

38. Any failure by the Attorney General to insist upon Anthem's compliance with any of the provisions of this Judgment shall not be deemed a waiver of any of the provisions hereof, and the Attorney General, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Judgment to be performed by Anthem.

39. If any clause, provision, or section of this Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Judgment and this Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

40. Nothing contained in this Judgment shall be construed to waive or limit any right of action by any consumer, person or entity, or by any local, state, federal or other governmental entity, except as provided by the Release herein.

41. Nothing in this Judgment shall prevent or restrict the use of this Judgment by the Attorney General in any action against Anthem for failure to comply with any of its provisions, or in the event that Anthem is in default of any of its terms and conditions. A default on the part of Anthem shall include any material breach of any of the terms or requirements of this Judgment. Nothing in this Judgment shall be construed to (i) exonerate any failure to comply with any of its provisions after the Effective Date of this Judgment, (ii) compromise or limit the authority of the Attorney General to initiate a proceeding for any failure to comply, or (iii) compromise the

authority of the Court or any other court of competent jurisdiction to impose any applicable remedies for any violation of this Judgment.

42. Nothing in this Judgment is intended to be and shall not be construed or deemed to be an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Anthem or of any fact or violation of any law, rule, or regulation. This Judgment is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind.

43. Anthem hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Judgment. Anthem has been represented by legal counsel and has been advised by their legal counsel of the meaning and legal effect of this Judgment.

44. This Judgment shall bind Anthem and its subsidiaries, affiliates, successors, future purchasers, acquiring parties, and assigns.

45. Within thirty (30) days of the Effective Date, Anthem will deliver a copy of this Judgment to (a) its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, and its General Counsel, and (b) its Board of Directors. In the event that any person assumes the role of Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, and its General Counsel, or becomes a member of the Board of Directors and such person has not been previously delivered a copy of this Judgment, Anthem shall deliver a copy of this Judgment to such person within thirty (30) days from which such person assumes such role or becomes a member of the Board of Directors and maintain a record of such.

46. With respect to existing subsidiaries and affiliates, which do not yet fall under the definition of Anthem as set forth in Paragraph 2(a), but which are wholly owned and Anthem intends to integrate and operate, Anthem shall within one hundred and eighty (180) days following the Effective Date of this Judgment develop a reasonable and appropriate implementation timetable for those subsidiaries and affiliates to achieve compliance with the provisions of this Judgment. For purposes of this provision, implementation shall mean (i) that Anthem or its subsidiaries and affiliates have taken the relevant measure(s) where technologically

feasible and otherwise reasonable, or have taken alternative measure(s) that alone or in the aggregate provide for substantially equivalent security, or (ii) that Anthem or its wholly owned, integrated, and operated subsidiaries and affiliates have developed a reasonable and appropriate plan to evaluate the technological and operational feasibility of the provisions of this Judgment. On a semiannual basis, Anthem will report to the Board of Directors regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

47. In the event that (1) Anthem acquires or merges with a subsidiary or affiliate after the Effective Date, (2) the subsidiary is wholly owned by Anthem, and (3) Anthem determines that it intends to wholly integrate and operate that subsidiary following the completion of an integration assessment, Anthem shall have one-hundred twenty (120) days from the data Anthem completes the integration assessment to develop and then implement an integration timetable regarding compliance with the terms of this Judgment. For purposes of this provision, implementation shall mean (i) that Anthem or its wholly owned, integrated, and operated subsidiaries and affiliates have taken the relevant measure(s) where technologically feasible and otherwise reasonable, or have taken alternative measure(s) that alone or in the aggregate provide for substantially equivalent security, or (ii) that Anthem or its wholly owned, integrated, and operated subsidiaries and affiliates have developed a reasonable and appropriate plan to evaluate the technological and operational feasibility of the provisions of this Judgment. On a semiannual basis, Anthem will report to the Board of Directors regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

48. The settlement negotiations resulting in this Judgment have been undertaken by the Parties in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

49. Anthem shall pay all court costs associated with the filing of this Judgment.

50. Anthem agrees that this Judgment does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and Anthem further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

51. This Judgment shall not be construed to waive any claims of sovereign immunity California may have in any action or proceeding.

52. This Judgment does not constitute an approval by the Attorney General of any of Anthem's past or future practices, and Anthem shall not make any representation to the contrary.

53. Anthem shall not participate directly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Judgment. Anthem shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Judgment.

54. Any notices or other documents required to be sent to the Parties pursuant to the Judgment shall be sent to the following address via first class and electronic mail, unless a different address is specified in writing by the party changing such address:

For the Attorney General:

Yen P. (TiTi) Nguyen
Consumer Protection Section—Privacy Unit
California Attorney General's Office
455 Golden Gate Ave., Suite 11000
San Francisco, California 94102-7004
Email: TiTi.Nguyen@doj.ca.gov

For Anthem:

Office of the General Counsel
Anthem, Inc.
220 Virginia Avenue
Indianapolis, IN 46204
Tel.: (800) 331-1476

with a copy to:

Craig Hoover
Michelle Kisloff
Allison Holt Ryan
Hogan Lovells US LLP

555 Thirteenth Street, NW
Washington, DC 20004
Tel.: (202) 637-5600
craig.hoover@hoganlovells.com
michelle.kisloff@hoganlovells.com
allison.holt-ryan@hoganlovells.com

55. This Court retains jurisdiction of this matter for purposes of construction, modification, and/or enforcement of this Judgment.

56. This Judgment shall take effect immediately upon entry thereof.

57. The clerk is directed to enter this Judgment forthwith.

ORDERED AND ADJUDGED at Alameda, California, this 30th day of September, 2020.

Judge of the Superior Court