IN THE FRANKLIN COUNTY COURT OF COMMON PLEAS
GENERAL DIVISION

State of Ohio ex rel. Attorney General Dave Yost,	**:**	
	:	**Case No. 19-CV-005610**
Plaintiff,		
	:	**Judge Jeffrey M. Brown**
vs.		
	:	
Premera Blue Cross,		
	:	
Defendant.		

AGREED ENTRY AND FINAL JUDGMENT ORDER

I. ORDER SUMMARY

1.1 Plaintiff, State of Ohio, by and through Ohio Attorney General Dave Yost ("the State") conducted an investigation and commenced this action pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services ("HHS") Regulations, 45 C.F.R. §§ 160 *et seq.* ("HIPAA"), and the Consumer Sales Practices Act, R.C. 1345.01 *et seq*.

1.2 Plaintiff and Defendant Premera Blue Cross ("PREMERA") consent to the entry of this Agreed Entry and Final Judgment Order ("Order") by the Court without the taking of proof and without trial or adjudication of any fact or law.

1.3 Plaintiff alleges that on March 17, 2015, PREMERA publicly announced a data security incident involving its computer network system which resulted in the unauthorized disclosure of certain consumers' personal information and protected health information.

1.4 Plaintiff and PREMERA agree that this Order does not constitute evidence or an admission regarding the existence or non-existence of any issue, fact, or violation of any law alleged by Plaintiff.

1.5 PREMERA recognizes and states that this Order is entered into voluntarily and that no promises or threats have been made by the Attorney General's Office or any member, officer, agent or representative thereof to induce it to enter into this Order, except as provided herein.

1.6 PREMERA waives any right they may have to appeal from this Order.

1.7 PREMERA further agrees that it will not oppose the entry of this Order on the grounds the Order fails to comply with Rule 65(d) of the Rules of Civil Procedure, and hereby waives any objections based thereon.

1.8 PREMERA further agrees that this Court shall retain jurisdiction of this action for the purpose of implementing and enforcing the terms and conditions of the Order and for all other purposes.

NOW, THEREFORE, it is hereby ORDERED, ADJUDGED, AND DECREED as follows:

II. PARTIES AND JURISDICTION

2.1 The State of Ohio, by and through Attorney General, Dave Yost, is the Plaintiff in this case.

2.2 PREMERA Blue Cross is a Washington non-profit corporation with its principal office located at 7001 220th St. SW, Building 1, Mountlake Terrace, Washington 98043.

2.3 The Court has jurisdiction over the subject matter of this action and jurisdiction over the parties to this action, and venue is proper in this Court.

2.4 Defendant, at all relevant times, has transacted business in the State of Ohio, including, but not limited to, Franklin County.

2.5 Jurisdiction is proper because PREMERA has transacted business within Ohio or has engaged in conduct impacting Ohio or its residents at all times relevant to the claims at issue.

2.6 This Order is entered pursuant to and subject to the Consumer Sales Practices Act, R.C. 1345.01 et seq.

III. DEFINITIONS

3.1 "COVERED SYSTEMS" shall mean all components, including but not limited to, assets, technology, and software, within the PREMERA NETWORK that are used to collect, process, transmit, and/or store PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION.

3.2 "CONSUMER PROTECTION LAWS" shall mean the Consumer Sales Practices Act, R.C. 1345.01 et seq.

3.3 "DESIGNATED PRIVACY OFFICIAL" shall mean the individual designated by PREMERA who is responsible for the development and implementation of the policies and procedures as required by 45 C.F.R. § 164.530(a).

3.4 "DESIGNATED SECURITY OFFICIAL" shall mean the individual designated by PREMERA who is responsible for the development and implementation of the policies and procedures as required by 45 C.F.R. § 164.308(a)(2).

3.5 "EFFECTIVE DATE" shall be July 11, 2019.

3.6 "ENCRYPTED" shall refer to the existing industry standard to encode or obscure data at rest or in transit. As of the EFFECTIVE DATE, the existing industry standard shall be AES 256-bit encryption or Transport Layer Security (TLS) 1.2, or their equivalents.

3.7 "GLBA" shall mean the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338.

3.8 "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services ("HHS") Regulations, 45 C.F.R. §§ 160 *et seq.*

3.9 "HIPAA SECURITY RULE" shall mean the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

3.10 "HIPAA PRIVACY RULE" shall mean the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

3.11 "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 a token or text message on a mobile phone; or (iii) Inherence factors, such as a biometric characteristic.

3.12 "MULTISTATE EXECUTIVE COMMITTEE" shall mean the Attorneys General of the States of Washington, Oregon, and California.

3.13 "PERSONAL INFORMATION" shall have the same meaning as listed in the SECURITY BREACH NOTIFICATION ACT.

3.14 "PREMERA" shall mean PREMERA Blue Cross, its parent and its directly or indirectly wholly-owned or controlled affiliates, subsidiaries and divisions, successors and assigns.[1]

3.15 "PREMERA NETWORK" shall mean all 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, operated, and/or controlled by PREMERA.

3.16 "PROTECTED HEALTH INFORMATION" shall mean "individually identifiable health information" as defined by the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology and Clinical Act (HITECH) and 45 C.F.R. § 160.103.

3.17 "SECURITY BREACH NOTIFICATION ACT" shall mean R.C. 1349.18 *et seq.* ("Private disclosure of security breach of computerized personal information data").

3.19 "SECURITY INCIDENT" shall mean any compromise to the confidentiality, integrity, or availability of a PREMERA information asset that includes PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION.

[1] For purposes of this definition, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity through majority ownership or voting power.

IV. INJUNCTIVE RELIEF

4.1 Application of Injunctions. The injunctive provisions of this Order shall apply to PREMERA and its officers, directors, and employees.

4.2 Injunctions. PREMERA shall engage in or refrain from engaging in the practices as identified in this Order.

4.3 **INTENTIONALLY LEFT BLANK**

4.4 **COMPLIANCE PROGRAM:**

a. PREMERA shall perform a comprehensive review and assessment of the effectiveness of its compliance program ("Compliance Program") pursuant to the terms of Paragraph 5.2.

b. PREMERA shall ensure that its Compliance Program is reasonably designed to ensure compliance with applicable federal and state laws related to data security and privacy.

c. PREMERA shall continue to employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Compliance Program (for ease, hereinafter referred to as the "Compliance Officer"). The Compliance Officer shall have the appropriate background or experience in compliance, including appropriate training in compliance with HIPAA, GLBA, and applicable state laws relating to privacy or data security.

d. The Compliance Officer shall continue to oversee PREMERA's Compliance Program, and shall function as an independent and objective body that reviews and evaluates compliance within PREMERA. The Compliance Officer shall develop a process for evaluating compliance risks and determining priorities, reviewing compliance plans, and ensuring follow-up to compliance issues identified occurs within a reasonable timeframe and that processes are in place for determining and implementing appropriate disciplinary and corrective actions when violations arise.

e. PREMERA shall continue to ensure that the Compliance Officer has direct access to the Chief Executive Officer and the Audit and Compliance Committee of the Board of Directors.

f. PREMERA shall ensure that its Compliance Program continues to receive the resources and support necessary to ensure that the Compliance Program functions as required and intended by this Order.

g. PREMERA may satisfy the implementation and maintenance of the Compliance Program and the safeguards required by this Order through review, maintenance, and, if necessary, updating of an existing compliance program or existing safeguards, provided that such existing compliance program and existing safeguards meet the requirements set forth in this Order.

4.5 **INFORMATION SECURITY PROGRAM:**

a. PREMERA may satisfy the implementation and maintenance of the Information Security Program and the safeguards and controls required by this Order through review, maintenance, and, if necessary, updating of an existing information security program or existing controls and safeguards, provided that such existing compliance program and existing safeguards and controls meet the requirements set forth in this Order.

b. PREMERA shall implement, maintain, regularly review and revise, and comply with a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, availability, and confidentiality of the PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that PREMERA collects, stores, transmits, and/or maintains.

c. PREMERA's Information Security Program shall document the administrative, technical, and physical safeguards appropriate to:

(i). The size and complexity of PREMERA's operations;

(ii). The nature and scope of PREMERA's activities; and

(iii). The sensitivity of the PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that PREMERA collects, stores, transmits, and/or maintains.

d. As part of its Information Security Program, PREMERA will not trust traffic on the PREMERA NETWORK. In order to trust the traffic, PREMERA shall:

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

(ii). Ensure that every device, user, and network flow is authorized and authenticated; and

(iii). Only allow access by users of the PREMERA NETWORK to the minimum extent necessary and require appropriate authorization and authentication prior to allowing any such access.

e. The Information Security Program shall be designed to:

(i). Protect the security, integrity, availability, and confidentiality of PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION;

(ii). Protect against any threats to the security, integrity, availability, or confidentiality of PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION;

(iii). Protect against unauthorized access to or use of PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION and minimize the likelihood of harm to any consumer;

(iv). Define and periodically reevaluate a schedule for retention of PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION and for its destruction when such information is no longer needed for business purposes;

(v). Restrict access within the PREMERA NETWORK based on necessity and job function, including but not limited to by restricting access to the PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION within the PREMERA NETWORK;

(vi). Assess the number of users on PREMERA's applications and retire any application with no active users and that no longer have a business purpose.

(vii). Restrict the ability of PREMERA employees and vendors to access the PREMERA NETWORK via personal devices (e.g., smartphones, tablets, personal laptops); PREMERA shall permit access only based on a business need. If required, the access shall be

restricted to only the data, systems, and other network resources required for the vendor's or employee's job. Any access to the PREMERA NETWORK via a personal device shall be reviewed on a regular basis to determine if the vendor's or employee's job function requires this access. Furthermore, this access shall be provided via a secured connection to the PREMERA NETWORK via VPN and MULTI-FACTOR AUTHENTICATION or other greater security safeguards; and

(viii). Restrict the ability of PREMERA's employees and vendors to use PREMERA assets (critical and non-critical) to access personal email, and social media, and file-sharing sites. For PREMERA's employees, PREMERA shall only permit access to non-PREMERA resources based on a business need.

f. PREMERA may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Order through review, maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that such existing information security program and existing safeguards meet the requirements set forth in this Order.

g. PREMERA shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (for ease, hereinafter referred to as the "Chief Information Security Officer"). The Chief Information Security Officer shall have the appropriate background or experience in information security and HIPAA compliance. PREMERA shall ensure that the Chief Information Security Officer is a separate position from the Chief Information Officer, and shall serve as PREMERA's DESIGNATED SECURITY OFFICIAL. The Chief Information Security Officer shall have direct access to the Chief Executive Officer and the Audit and Compliance Committee of the Board of Directors.

h. PREMERA shall ensure that the role of the Chief Information Security Officer includes directly advising PREMERA's Board of Directors, Chief Executive Officer, and Chief Information Officer on the management of PREMERA's security posture, the security risks faced by PREMERA, the security implications of PREMERA's decisions, and the adequacy of

PREMERA's Information Security Program. The Chief Information Security Officer shall meet with, and provide an oral or written update to: (1) the Board of Directors on at least an annual basis; (2) the Chief Executive Officer at least every two months; (3) the Chief Information Officer on at least a twice per month basis; and (4) the DESIGNATED PRIVACY OFFICIAL at least every two months. The Chief Information Security Officer shall inform the Chief Executive Officer, the Chief Information Officer, and the DESIGNATED PRIVACY OFFICIAL of any material unauthorized intrusion to the PREMERA NETWORK within forty-eight (48) hours of discovery of the intrusion. A material unauthorized intrusion is any intrusion to the PREMERA NETWORK that affects or may affect any PROTECTED HEALTH INFORMATION or PERSONAL INFORMATION**.**

i. PREMERA shall ensure that the Chief Information Security Officer and Information Security Program receive the resources and support necessary to ensure that the Information Security Program functions as intended by this Order.

j. PREMERA shall ensure that employees who are responsible for implementing, maintaining, or monitoring the Information Security Program, including but not limited to the Chief Information Officer and Chief Information Security Officer, have sufficient knowledge of the requirements of the Order.

k. At least once each year, PREMERA shall provide training on safeguarding and protecting consumer PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION to all employees who handle such information, and its employees responsible for implementing, maintaining, or monitoring the Information Security Program. PREMERA's Information Security Program shall be designed and implemented to ensure the appropriate and timely identification, investigation of, and response to SECURITY INCIDENTS.

l. PREMERA shall provide its DESIGNATED PRIVACY OFFICIAL with appropriate training to ensure the official is able to implement the requirements of and ensure compliance with the HIPAA PRIVACY AND SECURITY RULES.

m. PREMERA shall provide its DESIGNATED SECURITY OFFICIAL with appropriate training to ensure the official is able to implement the requirements of and ensure compliance with the HIPAA SECURITY RULE.

n. PREMERA shall maintain a written incident response plan to prepare for and respond to SECURITY INCIDENTS. PREMERA shall revise and update this response plan, as necessary, to adapt to any changes to the PREMERA NETWORK and its COVERED SYSTEMS. Such a plan shall, at a minimum, identify and describe the following phases:

(i). Preparation;

(ii). Investigation, 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 (Lessons Learned).

o. For each SECURITY INCIDENT, PREMERA shall create a report that includes a description of the SECURITY INCIDENT and PREMERA's response to that SECURITY INCIDENT ("Security Incident Report"). The Security Incident Report shall be made available for the Third-Party Assessment as described in Paragraph 5.1.

p. PREMERA shall make reasonable efforts to ensure that any service providers or vendors it employs that handle PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION shall (1) have safeguards in place to protect any of PERSONAL INFORMATION, or PROTECTED HEALTH INFORMATION, and (2) notify PREMERA promptly after discovering any potential compromise of the confidentiality, integrity, or availability of PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that is held, stored or processed by the service provider or vendor on behalf of PREMERA.

4.6 **PERSONAL INFORMATION AND PROTECTED HEALTH INFORMATION SAFEGUARDS AND CONTROLS:**

a. On an annual basis, PREMERA shall review, and if necessary update, its data retention policies to ensure that its PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION within the PREMERA NETWORK is only collected, stored, maintained, and/or processed to the extent necessary to accomplish the intended purpose in using such information.

b. PREMERA shall implement, maintain, regularly review and revise, and comply with policies and procedures to ENCRYPT PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION, whether the information is transmitted electronically over a network or is stored on any media, whether it be static, removable, or otherwise.

4.7 **SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS:**

a. Asset Inventory and Managing Critical Assets:

(i). PREMERA shall, within one hundred and eighty days (180) days of the EFFECTIVE DATE of this Order, implement and maintain a configuration management database that contains an asset inventory for all known Critical Assets that identifies: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the PREMERA NETWORK; (e) whether the asset is a Critical Asset; and (f) the date that each security update or patch was applied. PREMERA shall apply the highest rating it uses for any asset that either it uses to collect, store, transmit, or use PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION ("Critical Assets").

(ii). PREMERA shall, within one year of the EFFECTIVE DATE of this Order, implement and maintain an asset inventory for all assets that identifies: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the PREMERA NETWORK; (e) whether the asset is a Critical Asset; and (f) the date that each security update or patch was applied.

b. Mapping and Encryption of Sensitive Data:

(i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE, identify

and map all locations where PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION is collected, stored, received, maintained, processed or transmitted within the PREMERA network. PREMERA shall perform this identification and mapping procedure at least annually. Any such documentation must be made available for inspection for the Assessment as described in Paragraph 5.1.

(ii). PREMERA shall ensure that electronic PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION that is stored at rest or is in transmission is ENCRYPTED except where PREMERA determines that ENCRYPTION is not reasonable and appropriate and it documents the rationale for this decision.

c. Segmentation: PREMERA shall implement and maintain segmentation protocols and related policies that are reasonably designed to properly segment the PREMERA NETWORK, which shall, at a minimum, ensure system functionality and performance to meet business needs while also mitigating exposure to the enterprise network in the event of an attack or malicious intruder access. Additionally, PREMERA shall regularly evaluate, and as appropriate, restrict and disable any unnecessary ports of service on the PREMERA NETWORK.

d. Penetration Testing: PREMERA shall engage a third-party vendor to perform an annual penetration test to the PREMERA NETWORK, and shall ensure any risks or vulnerabilities identified are risk assessed, prioritized, and addressed under PREMERA'S Information Security Program. The parties understand and agree that addressing a risk may include remediation or alternate risk mitigation efforts based on the risk assessment in Paragraph 4.7(e).

e. Risk Assessment: PREMERA shall conduct an accurate and thorough risk assessment on any material risks and/or vulnerabilities identified by its internal auditors or through penetration testing as required by Paragraph 4.7(d) within thirty (30) days of identification of the risk or vulnerability to the PREMERA NETWORK and its COVERED SYSTEMS. PREMERA shall rate each vulnerability on a risk-based rating scale developed by PREMERA that takes into account cybersecurity best practices and risk to PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION. PREMERA shall ensure that risks or vulnerabilities that threaten the

safeguarding or security of any PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION maintained on the PREMERA NETWORK shall be addressed and remediated as expeditiously as possible. PREMERA shall document in writing any decision not to address a risk or vulnerability that threatens the safeguarding or security of any PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION maintained on the PREMERA NETWORK.

(i). The risk assessment shall include an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held as required by HIPAA Security Rule, 45 C.F.R. § 164.308(a)(1)(ii)(A).

(ii). PREMERA shall implement and maintain a corresponding risk-assessment program designed to identify and assess risks to the PREMERA NETWORK. In cases where PREMERA deems quantitative risk to be acceptable, PREMERA shall generate and retain a report demonstrating how such risks are to be managed in consideration of the risk to PERSONAL INFORMATION and PROTECTED HEALTH INFORMATION, and the cost or difficulty in implementing effective countermeasures. All reports shall be maintained by the Chief Information Security Officer and be available for inspection by its DESIGNATED PRIVACY OFFICIAL, and the Third-Party Assessor described in Paragraph 5.1 of this Order.

f. Secure Network Communications: PREMERA shall implement and maintain controls that filter incoming emails for potential phishing attacks or other fraudulent emails and that establish strong peer-to-peer communications between its employees and vendors. In addition, PREMERA will secure external communications to limit the ability of an attacker or malicious intruder to communicate from the PREMERA NETWORK to unknown IP addresses.

g. Access Control and Account Management: PREMERA shall implement and maintain appropriate controls to manage access to accounts and shall take into account whether the user is on a PREMERA device or a non-PREMERA device, such as a personal device, and whether

the user is physically located at a PREMERA site or connecting to PREMERA through a remote connection.

(i). PREMERA shall, within nine (9) months of the EFFECTIVE DATE, implement and maintain appropriate controls to manage access to, and use of, all administrator, service, and vendor accounts with access to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION. Such controls shall include, without limitation, (a) strong passwords, (b) password confidentiality policies, (c) password-rotation policies, (d) MULTI-FACTOR AUTHENTICATION or any other equal or greater authentication protocol for identity management, and (e) appropriate safeguards for administrative level passwords.

(ii). PREMERA shall implement and maintain appropriate controls to manage access to, and use of, all PREMERA employee user accounts with access to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION.

(iii). PREMERA shall implement and maintain appropriate administrative processes and procedures to store and monitor the account credentials and access privileges of employees who have privileges to design, maintain, operate, and update the PREMERA NETWORK.

(iv). PREMERA shall implement and maintain appropriate policies for the secure storage of account passwords, including, without limitation, hashing passwords stored online using an appropriate hashing algorithm that is not vulnerable to a collision attack, and an appropriate salting policy.

(v). PREMERA shall implement and maintain adequate access controls, processes, and procedures, the purpose of which shall be to grant access to the PREMERA NETWORK only if the user is properly authorized and authenticated.

(vi). PREMERA shall immediately disable access privileges for all persons whose access to the PREMERA NETWORK is no longer required or appropriate. PREMERA shall limit access to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION by persons accessing the PREMERA NETWORK on a least-privileged basis.

(vii). PREMERA shall regularly inventory the users who have access to the PREMERA NETWORK in order to review and determine whether or not such access remains necessary or appropriate. PREMERA shall regularly compare employee termination lists to user accounts to ensure access privileges have been appropriately terminated. At a minimum, such review shall be performed on a quarterly basis. When the privileges, including for any disabled accounts, are determined to be no longer necessary for any business function, PREMERA shall terminate access privileges for those accounts.

(viii). PREMERA shall implement and maintain network endpoint (e.g., devices and PCs) security by using network access controls to identify devices accessing the PREMERA NETWORK, such as an identity-based network access controller or a similar product.

h. File Integrity and End-point Monitoring: PREMERA shall deploy and maintain controls designed to provide near real-time and/or real-time notification of unauthorized access to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION. PREMERA shall, within six (6) months from the EFFECTIVE DATE of this Order, deploy and maintain controls designed to provide near real-time or real-time notification of modifications to any applications or systems that either contain or provide access to PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION.

i. Controlling Permissible Applications: For servers in the PREMERA NETWORK, PREMERA shall deploy and maintain controls within one year of the EFFECTIVE DATE that are designed to block and/or prevent the execution of unauthorized applications within the PREMERA NETWORK, as prescribed in the implementation standards of the HITRUST framework. For clients (e.g., desktops, laptops, tablets), PREMERA shall maintain the controls prescribed in the implemented HITRUST framework designed to block and/or prevent the execution of unauthorized applications within the PREMERA NETWORK. Additionally, the controls will provide alerts when unauthorized applications attempt to execute on the PREMERA NETWORK.

j. Logging and Monitoring: PREMERA shall maintain reasonable policies, procedures, and controls the purpose of which shall be to properly monitor and log activities on the PREMERA NETWORK.

(i). PREMERA shall ensure that logs are automatically processed and aggregated, and then actively monitored and analyzed in real time or near real time.

(ii). PREMERA shall test at least twice per year, any software, hardware, or service used pursuant to this paragraph, to ensure it is properly configured, and regularly updated and maintained to ensure that all COVERED SYSTEMS are adequately logged and monitored.

k. Change Control: PREMERA shall implement and maintain policies and procedures reasonably designed to manage and document changes to the PREMERA NETWORK.

l. Updates/Patch Management: PREMERA shall maintain, keep updated, and support the software on the PREMERA NETWORK taking into consideration the impact a software update will have on data security in the context of the entire PREMERA NETWORK and its ongoing business and network operations, and the scope of the resources required to maintain, update and support the software. PREMERA shall deploy and maintain reasonable controls to ensure that risks posed by software no longer supported by the manufacturer are adequately addressed and reasonably mitigated.

V. ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY GENERAL

5.1 Information Security Assessment:

a. PREMERA shall, for a period of three years (3) after the EFFECTIVE DATE of this Order, obtain an annual information security assessment and report from a third-party professional ("Third-Party Assessor") using procedures and standards generally accepted in the profession ("Third-Party Assessment"), commencing within one (1) year after the EFFECTIVE DATE of this Order. The Third-Party Assessor's report on the Third-Party Assessment shall:

(i). Set forth the specific administrative, technical, and physical safeguards maintained by PREMERA;

(ii). Explain the extent to which such safeguards are appropriate in light of PREMERA's size and complexity, the nature and scope of PREMERA's activities, and the sensitivity of the PERSONAL INFORMATION or PROTECTED HEALTH INFORMATION maintained by PREMERA;

(iii). Assess and certify the extent to which the administrative, technical, and physical safeguards that have been implemented by PREMERA meet the requirements of the Information Security Program;

(iv). Assess and certify the extent to which PREMERA is complying with the requirements of the Information Security Program;

(v). Specifically review and evaluate the reasonableness of any decision to not encrypt PERSONAL INFORMATION and PERSONAL HEALTH INFORMATION, in compliance with Paragraph 4.7(b).

(vi). Specifically review and evaluate PREMERA's response to SECURITY INCIDENTS in the Security Incident Report (see Paragraph 4.5(o)); and

(vii). Specifically review and evaluate PREMERA's compliance with the penetration testing requirements set forth in Paragraph 4.7(d); the risk assessment requirements set forth in Paragraph 4.7(e); the logging and monitoring requirements set forth in Paragraph 4.7(j); the change control requirements set forth in Paragraph 4.7(k); and the updates/patch management requirements set forth in Paragraph 4.7(l).

b. The Third-Party Assessor shall be a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; have at least five (5) years of experience evaluating the effectiveness of computer system security or information system security; and must be approved by the MULTISTATE EXECUTIVE COMMITTEE.

c. Each Third-Party Assessment must be completed within sixty (60) days after the end of the reporting period to which the Third-Party Assessment applies. PREMERA shall provide a copy

of the Third-Party Assessor's Report on the Third-Party Assessment to the Washington Attorney General's Office within thirty (30) days of the completion of the report.

d. The State of Washington shall, to the extent permitted by the laws of the State of Washington, treat such Third-Party Assessor's Report as exempt from disclosure under the relevant public records laws.

e. The Washington Attorney General's Office may provide a copy of the Third-Party Assessor's Report received from PREMERA to another Attorney General's Office upon request, and that Attorney General shall, to the extent permitted by the laws of Ohio, treat such Third-Party Assessor's Report as exempt from disclosure under the relevant public records laws.

5.2 Compliance Program Assessment: Within one-hundred-and-eighty (180) days of the EFFECTIVE DATE of this Order, PREMERA shall conduct an assessment of the structure of and personnel responsible for PREMERA's Compliance Program (the "Compliance Program Assessment"). The Compliance Program Assessment required by this paragraph shall be conducted by a third-party professional (the "Compliance Program Assessor").

a. The Compliance Program Assessor shall use procedures and standards generally accepted in the profession.

b. The Compliance Program Assessor shall:

(i). Examine the effectiveness of the PREMERA's Compliance Program;

(ii). Examine the independence and effectiveness of the structure of employees responsible for PREMERA's Compliance Program;

(iii). Identify any potential conflicts-of-interest that may hinder PREMERA's obligation to comply with state and federal laws related to data security and privacy; and

(iv). Examine PREMERA's HIPAA Risk Analysis Assessment and Mitigation Plan, as required by 45 C.F.R. § 164.308(a)(1)(ii)(A) and relevant guidelines provided by the Office for Civil Rights.

c. The findings of the Compliance Program Assessment shall be documented in a report (the "Compliance Program Assessor's Report"). PREMERA shall provide a copy of the

Compliance Program Assessor's Report to the Washington Attorney General's Office within thirty (30) days of the completion of the Compliance Program Assessment.

d. The State of Washington shall, to the extent permitted by the laws of the State of Washington, treat such Compliance Program Assessor's Report as exempt from disclosure under the relevant public records laws.

e. The Washington Attorney General's Office may provide a copy of the Compliance Program Assessor's Report received from PREMERA to the Ohio Attorney General's Office upon request, and that Attorney General shall, to the extent permitted by the laws of Ohio, treat such Compliance Program Assessor's Report as exempt from disclosure under the relevant public records laws.

5.3 PREMERA will make reasonable good faith efforts to address any concerns and implement recommendations made by the Third-Party Assessor or the Compliance Assessor.

VI. DOCUMENT RETENTION

6.1 PREMERA shall retain and maintain the reports, records, information and other documentation required by this Order for a period of no less than three (3) years after the document is finalized, last edited, or last used.

VII. PAYMENT TO THE STATES

7.1 No later than thirty (30) days after the EFFECTIVE DATE, PREMERA shall pay a total of Ten Million Dollars ($10,000,000.00) to the Attorneys General. This amount is to be divided and paid by PREMERA directly to the Attorneys General in amounts to be designated by and in the sole discretion of the MULTISTATE EXECUTIVE COMMITTEE.[2] Said payment shall be used by the Ohio Attorney General for additional consumer relief; attorneys' fees and other costs of investigation and litigation; or to be placed in, or applied to, consumer protection enforcement funds, including future consumer protection enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for any lawful

[2] The amount due to the Ohio Attorney General under this paragraph is Sixty-Seven Thousand Seven Hundred Ninety-One Dollars and Ninety-Two Cents ($67,791.92).

purpose, at the sole discretion of the Attorney General.

VIII. RELEASE

8.1 Following full payment of the amount due under this Order, the Ohio Attorney General shall release and discharge PREMERA from all civil claims that the Attorney General has or could have brought under the Consumer Sales Practices Act, R.C. 1345.01 *et seq.*; the SECURITY BREACH NOTIFICATION ACT, R.C. 1349.18 *et seq.*, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services ("HHS") Regulations, 45 C.F.R. §§ 160 *et seq.*, arising out of PREMERA's conduct and the Attorney General's investigation of the data security incident first publicly announced March 17, 2015. Nothing contained in this paragraph shall be construed to limit the ability of the Ohio Attorney General to enforce the obligations that PREMERA has under this Order. Further, nothing in this Order shall be construed to create, waive, or limit any private right of action or any action brought by any state agency other than the Attorney General.

8.2 The obligations and other provisions of this Order set forth in Sections 4.5 and 4.7 shall expire at the conclusion of the five (5) year period after the EFFECTIVE DATE of this Order, unless they have expired at an earlier date pursuant to their specific terms. The obligations and other provisions of this Order set forth in Paragraphs 4.4 and 4.6 shall expire at the conclusion of the ten (10) year period after the EFFECTIVE DATE of this Order, unless they have expired at an earlier date pursuant to their specific terms. Other sections and paragraph with specified time periods shall expire as detailed in those sections and paragraphs. Nothing in this paragraph should be construed or applied to excuse PREMERA from its obligation to comply with all applicable state and federal laws, regulations and rules.

8.3 Notwithstanding any term of this Order, any and all of the following forms of liability are specifically reserved and excluded from the release as to any entity or person, including PREMERA:

a. Any criminal liability that any person or entity, including PREMERA, has or may have to the States.

b. Any civil or administrative liability that any person or entity, including PREMERA, has or may have to the States 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.

IX. MEET AND CONFER

9.1 If any Attorney General determines that PREMERA has failed to comply with any of Sections IV and V of this Order, and if in the Attorney General's sole discretion the failure to comply with this Order does not threaten the health or safety of the citizens of the Attorney General's State and/or does not create an emergency requiring immediate action, the Attorney General will notify PREMERA in writing of such failure to comply and PREMERA shall have thirty (30) days from receipt of such written notice to provide a good faith written response to that Attorney General, including either a statement that PREMERA believes it is in full compliance or otherwise a statement explaining how the violation occurred, how it has been addressed or when it will be addressed, and what PREMERA will do to make sure the violation does not happen again. The Attorney General may agree to provide PREMERA more than thirty (30) days to respond.

9.2 Nothing herein shall be construed to exonerate any failure to comply with any provision of this Order, or limit the right and authority of an Attorney General to initiate a proceeding for any failure to comply with this Order after receiving the response from PREMERA

described in Paragraph 9.1, if the Attorney General determines that an enforcement action is in the public interest.

X. ENFORCEMENT

10.1 Violation of any of the injunctions contained in this Order, as determined by the Court, shall constitute a violation of an injunction for which civil penalties may be sought by the Attorney General as provided by law.

10.2 This Order is entered pursuant to R.C. 1345.01 *et seq.* Jurisdiction is retained for the purpose of enabling any party to this Order with or without the prior consent of the other party to apply to the Court at any time for enforcement of compliance with this Order, to punish violations thereof, or to modify or clarify this Order.

10.3 Under no circumstances shall this Order or the name of the State of Ohio, the Office of the Attorney General, Consumer Protection Division, or any of their employees or representatives be used by PREMERA in connection with any selling, advertising, or promotion of products or services, or as an endorsement or approval of PREMERA's acts, practices or conduct of business.

10.4 This Order shall not bar the Ohio Attorney General or any other governmental entity from enforcing laws, regulations, or rules against PREMERA for conduct subsequent to or otherwise not covered by this Order. Further, nothing in this Order shall be construed to limit the ability of the Ohio Attorney General to enforce the obligations that PREMERA has under this Order.

10.5 Nothing in this Order shall be construed as relieving PREMERA of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Order be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

10.6 PREMERA shall deliver a copy of this Order to, and otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, Compliance Officer, DESIGNATED PRIVACY OFFICIAL, DESIGNATED SECURITY OFFICIAL, Chief Legal Officer, and its Board of Directors within (30) days of the EFFECTIVE DATE. To the extent PREMERA hires or replaces any of the above listed officers, counsel or Directors, PREMERA shall deliver a copy of this Order to their replacements within thirty (30) days from the date on which such person assumes his/her position with PREMERA.

10.7 No court costs, if any, shall be taxed upon the Attorney General. To the extent there are any court costs associated with the filing of this Order, PREMERA shall pay all such court costs.

10.8 PREMERA shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Order or for any other purpose that would otherwise circumvent any term of this Order. PREMERA shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Order.

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

10.10 This Order shall not be construed to waive any claims of sovereign immunity Ohio may have in any action or proceeding.

10.11 If any portion of this Order is held invalid by operation of law, the remaining terms of this Order shall not be affected and shall remain in full force and effect.

10.12 Whenever PREMERA shall provide reports to the Washington Attorney General under Section V of this Order, those requirements shall be satisfied by sending the report to: ATTN:

Tiffany Lee and Andrea Alegrett, Assistant Attorneys General, Consumer Protection Division, Office of the Attorney General, 800 Fifth Avenue #2000, Seattle, WA 98104.

10.13 Any notice or report provided by the Attorney General to PREMERA under Section IX of this Order shall be satisfied by sending notice to: Chief Legal Officer, Premera Blue Cross, 7001 220th St., SW, MS 316, Mountlake Terrace, WA 98043.

10.14 All documents to be provided under this Order shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. The parties may update their designee or address by sending written notice to the other party informing it of the change.

10.15 Jurisdiction is retained by the Court for the purpose of enabling any party to the Order to apply to the Court at any time for such further orders and directions as may be necessary or appropriate for the construction or the carrying out of this Order, for the modification of any of the injunctive provisions hereof, for enforcement of compliance herewith, and for the punishment of violations hereof, if any.

IT IS SO ORDERED, ADJUDGED, AND DECREED.

APPROVED AND AGREED TO BY:

PLAINTIFF

Dave Yost
Attorney General of the State of Ohio

By: */s/ Michael S. Ziegler*
Michael S. Ziegler (0042206)
Principal Assistant Attorney General

By: */s/ Melissa Szozda Smith*
Melissa Szozda Smith (0083551)
Assistant Chief

Office of the Ohio Attorney General - Consumer Protection Section
30 East Broad Street, 14th Floor
Columbus, Ohio 43215
614/466-3980
866/404-4121 (facsimile)
Michael.Ziegler@OhioAttorneyGeneral.gov

Date: July 11, 2019

Attorneys for Plaintiff

DEFENDANT

PREMERA BLUE CROSS

By:

/s/ Tim McMichael, per written authorization, by Michael S. Ziegler
Tim McMichael
Assistant General Counsel – Director of Litigation / SI
Premera Blue Cross

Date: July 10, 2019

For PREMERA BLUE CROSS

By:

/s/ Theodore J. Kobus III, per written authorization, by Michael S. Ziegler
THEODORE J. KOBUS III
Baker & Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111-0100

Date: July 10, 2019

Counsel for Defendant

Approved as to form:

By:

/s/ Patrick H. Haggerty, per written authorization, by Michael S. Ziegler

PATRICK H. HAGGERTY, Bar #0075715
Baker & Hostetler LLP
312 Walnut St., Suite 3200
Cincinnati, OH 45202
513/929-3412
phaggerty@bakerlaw.com

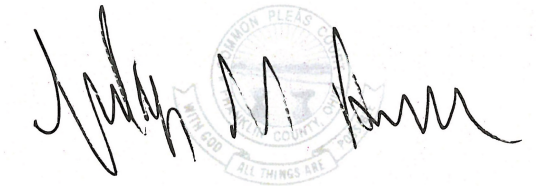
Date: July 10, 2019

Local Counsel for Defendant

Franklin County Court of Common Pleas

Date:	07-22-2019
Case Title:	STATE OF OHIO EX REL ATTORNEY GENERAL -VS- PREMERA BLUE CROSS
Case Number:	19CV005610
Type:	AGREED ORDER

It Is So Ordered.



/s/ Judge Jeffrey M. Brown

Court Disposition

Case Number: 19CV005610

Case Style: STATE OF OHIO EX REL ATTORNEY GENERAL -VS- PREMERA BLUE CROSS

Case Terminated: 18 - Other Terminations

Final Appealable Order: No