July 18th, 2022

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Sir:

I am writing to notify you of a privacy incident affecting a downstream business associate of Premera Blue Cross as required under RCW 19.255.010 and 42.56.590. Community Care Health Network, LLC d/b/a Matrix Medical Network ("Matrix") is a Premera business associate that provides in-home medical assessments.

Matrix was notified on 4/29/2022 by OneTouchPoint, Inc. ("OTP"), their printing and mailing business associate that they were the target of a ransomware attack which initiated on 4/27/2022. They confirmed that there was unauthorized access to some of their servers. Once OTP learned of the event, they engaged third-party forensic specialists to investigate the event and took actions to enhance its existing security measures to help ensure that a similar incident does not occur in the future. OTP engaged to conduct negotiations with the attackers and a settlement was reached.

OTP's risk analysis concluded that forensics evidence could not be obtained to prove the threat actors did or did not access Premera' s data in their Hartland data center due to corruption in a folder not allowing them to confirm the status. Out of an abundance of caution, OTP identified that 1314 Premera members may have been affected by the Black Basta ransomware encryption. Premera received an affected member list, verified and identified the state of residence on 6/20/2022. Of the 1314 total potentially members, 1303 are residents of Washington State. All members are Medicare Advantage plan participants. Based on the letters mailed to our members by OPT, the following PHI may have become visible: name, member ID, address, health plan name and address, medical information , provider name and address. No billing, financial, SSN or date of birth information were potentially disclosed.

OTP will be providing individual notification letters to affected members starting the week of July 11th, 2022 (please see attached) as well as making required State and Federal regulatory notifications during that week.

To help prevent something like this from happening in the future, OTP is taking additional steps to implement additional safeguards and are reviewing policies and prociedures relating to data privacy and security.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Chris Brandt
Privacy Official and Senior Privacy Manager
Premera Blue Cross
Columbia Bldg M33B76
7001 220th St SW
Mountlake Terrace, WA 98043
(425)918-5531
Christopher.Brandt@Premera.com

OneTouchPoint

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>> <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Notice of Data [Event/Breach]

Dear <<Name 1>> <<Name 2>>:

OneTouchPoint, Inc. ("**OTP**") writes to notify you of an incident that may affect the privacy of some of your information. OTP is a vendor who provides printing and mailing services to various health insurance carriers and medical providers. To provide these services, OTP was provided certain information related to a health assessment you received. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? On April 28, 2022, OTP discovered encrypted files on certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to certain of our servers beginning on April 27, 2022. On June 1, 2022, we learned that we would be unable to determine what specific files the unauthorized actor viewed within our network. OTP provided a summary of our investigation to our customers beginning on June 3, 2022. OTP later determined that the impacted systems contained certain information related to you. While we were unable to say definitively if your information was accessed by the unauthorized actor, we are notifying you of the event in an abundance of caution. OTP has seen no evidence of misuse of any information related to this incident.

What Information Was Involved? OTP determined that the following information related to you was present on the impacted OTP servers: your name and <data elements>. Your Social Security number was not impacted by this event.

What We Are Doing. OTP takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. We reported this incident to the law enforcement, and we are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security.

What You Can Do. OTP encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* for additional details on how to take steps to protect your information, should you feel it is necessary to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call XXX-XXX-XXXX, Monday through Friday, from X:00 a.m. to X:00 p.m. Eastern Time. Additionally, you can write to us at OneTouchPoint, Inc., Attention: Incident Response, 1225 Walnut Ridge Drive, Hartland, Wisconsin 53029.

OTP takes the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you

Sincerely,

Mike Fox
Chief Information Officer OneTouchPoint, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "**fraud alert**" on a credit file at no cost. An initial fraud alert is a 1- year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit- report-services/	https://www.experian.com/help/	https://www.transunion.com/credit- help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade

Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "**prescreened**" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.