SWEDISH

May 29, 2020

Sent Via Email at SecurityBreach@atg.wa.gov

Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

RE: Notice of Data Security Incident

Dear Attorney General Ferguson:

This letter is to provide you notice of a cybersecurity incident that we recently became aware of.

1. Nature of the security incident.

On January 15, 2020, it was discovered that Swedish Health Services' ("Swedish") network was breached by an unauthorized user. Prompt investigation revealed credentials belonging to a small number of Providence Health & Services ("Providence") caregivers (Swedish is affiliated with Providence and purchases certain shared services from them including cybersecurity services) were obtained by the unauthorized user, including some who support programs involving Swedish caregivers. An outside cybersecurity firm was engaged and subsequently conducted a thorough investigation of the incident. On or about May 1, 2020, the cybersecurity firm delivered their report, informing Swedish that an email account had been compromised. This email account contained a spreadsheet with demographic information, compensation data, and Social Security numbers of 12,901 Swedish caregivers who were employed at the time the file was created on or about August 19, 2019. At this time there is no indication the compromised information has been utilized by any bad actors.

2. Number of Washington residents affected.

Approximately 12,573 residents of Washington were affected by this incident. Swedish notified the affected Washington residents on May 29, 2020 via regular mail (a copy of which is attached to this letter).

3. Steps taken in response to the incident.

As part of our mitigation efforts, Swedish pushed out a mandatory password change program to tighten security regarding email accounts. Additionally, multi-factor authentication has been implemented for Microsoft Office 365; our enterprise suite of cloud based collaboration tools, as

well as for Citrix, our enterprise portal used for securely accessing our network and applications remotely.

4. Contact Information.

Swedish remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 206-215-2613 or by email at Jennifer.Mcaleer@Swedish.org. Please let me know if you have any questions.

Sincerely Yours,

Jennifer McAleer
Chief Compliance and Privacy Officer
Swedish Health Services

Attachment: Sample Notification Letter

SWEDISH

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

SEQ
CODE 2D
Ver SWE

To Enroll, Please Call:
1-833-579-1103
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

May 29, 2020

Dear <<First Name>> <<Last Name>>,

I am writing to share important information about an incident that may impact you. This letter outlines information about what occurred and how you can sign-up for free identity theft protection.

Summary of Incident: As part of our ongoing review, we discovered that on January 15, 2020 our network was breached by an unauthorized user. We immediately took measures to restore network protection and safeguard against further unauthorized access. We promptly initiated an investigation and determined that the unauthorized user obtained the login credentials of a small number of Providence Health & Services caregivers, including some who support programs involving Swedish caregivers. We engaged a cybersecurity firm to thoroughly investigate the extent of the incident.

The firm delivered a report of the multifaceted incident to us on May 1, 2020. The report indicates that your personal information was contained in a file used by human resources and then subsequently illegally downloaded by an unauthorized user on December 18, 2019. The file included the following fields of sensitive information:

> Full name, nickname, employee identification number, street address, email address, gender, date of birth, age, Social Security number, Equal Employment Opportunity class, ethnicity, personal phone number, employment status, date of hire, adjusted hire date, work anniversary date, retirement date, position description information and date assigned, department name and location, job code, class and title, exempt/non-exempt status, work schedule, supervisor name, union and bargaining unit information, pay grade, pay rate, and pay range.

The firm's report indicates that there is no evidence that your information has been used inappropriately. Still, we sincerely regret the incident occurred.

Unrelated unemployment fraud scheme: You may have heard of the large scale unemployment fraud scheme currently targeted at residents of Washington State. At this time we do not believe that these two situations are related, since those impacted by the unemployment fraud scheme include many individuals who have no ties to Swedish or Providence Health & Services. If you do receive notification that someone has filed an unemployment claim on your behalf and you believe it was done fraudulently, we recommend that you contact the Washington State Employment Security Department by following this link https://esd.wa.gov/unemployment/unemployment-benefits-fraud or by calling the Office of Special Investigations at 800-246-9763.

Take action to sign-up for free identity theft protection services: In consideration of the incident, we offer you a one-year membership of identity theft protection services through ID Experts® at no cost to you. ID Experts, a data breach and recovery services firm, offers MyIDCare™ services including: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and comprehensive ID theft recovery services. As part of the services, MyIDCare will also assist in resolving matters if your information is compromised.

To accept MyIDCare services at no cost, please visit https://app.myidcare.com/account-creation/protect or call **1-833-579-1103**. Please provide the enrollment code at the top of this letter. MyIDCare experts are available Monday through Friday

from 6 am to 6 pm Pacific Time. Please note, you must enroll in the program by **August 31, 2020** in order to take advantage of the offer for free MyIDCare services.

As a precautionary measure, we recommend that you protect yourself against possible fraud and identity theft by reviewing your account statements and monitoring credit reports closely. If you observe any suspicious activity with an account, promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission (FTC). If you are interested in more information about identity theft, visit https://www.ftc.gov/idtheft or call **1-877-ID-THEFT (1-877-438-4338)**. You can also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. Please visit http://www.annualcreditreport.com, call **1-877-322-8228**, or complete an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com.

You may also purchase your credit reports by contacting the national credit reporting agencies. Contact information for the national credit reporting agencies is:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: Consider placing a fraud alert on your credit reports. A fraud alert notifies creditors of potential unauthorized activity on your accounts and requests that the creditor contact you before establishing a new account in your name. Your first fraud alert is free and will stay on your credit file for at least 90 days. To place a fraud alert on your credit file, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze (or security freeze) on your credit files. A credit freeze prohibits any new credit account to be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. Please note, if you set up a credit freeze, potential creditors will not be able to view your credit report unless you lift the freeze and may delay your ability to obtain credit. Unlike a fraud alert, you have to place a credit freeze on your credit file with each credit reporting company. The instructions for establishing a credit freeze differ from state to state, so please contact the credit reporting companies as specified below for more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to start a credit freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security Number
3. Date of birth
4. If you have moved in the past five (5) years, (provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft (include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft)

The credit reporting agencies have three (3) business days to place a credit freeze on your file after you make a request. They will send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal of the credit freeze. To remove the credit freeze in order to allow a specific access to your credit file, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the credit freeze as well as the identity of the individual you would like to receive your credit report or the specific period of time you want your credit file to available. The credit reporting agencies have three (3) business days after receiving your request to remove the credit freeze for those identified entities or for the specified period of time.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/learnmore or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

For further information and assistance, please contact Jennifer McAleer, Swedish Chief Compliance and Privacy Officer, at Compliance@Swedish.org or by phone at 206-215-2613. Again, we are sorry that this occurred. Please let us know how we can support you through this unfortunate incident.

Sincerely Yours,

Jennifer McAleer
Chief Compliance & Privacy Officer
Swedish Health Services

SEQ
CODE 2D