Joseph Fusz
312.821.6141 (Direct)
Joseph.Fusz@wilsonelser.com

June 13, 2024

Via U.S. Mail

Attorney General Lawrence Wasden
Office of the Attorney General
700 W. Jefferson Street, Suite 210
P.O. Box 83720
Boise, Idaho 83720-0010

RE: Notice of Cybersecurity Incident Involving Highland Health Systems

Dear Attorney General Wasden:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Highland Health Systems located at 331 East 8th Street, Anniston, AL with respect to a data security incident that it recently experienced. By providing this notice, Highland Health Systems does not waive any rights or defenses regarding the applicability of Idaho law or personal jurisdiction. Highland Health Systems takes the security and privacy of the information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of individuals being notified, and the steps that Highland Health Systems has taken in response to the Incident.

1. Nature of the Incident

On July 3, 2023, Highland Health Systems detected unusual activity on our network. Upon discovery of this incident, Highland Health Systems immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. During the forensic investigation, Highland Health Systems found evidence that some of our files were accessed by an unauthorized actor.

Based on these findings, Highland Health Systems began a lengthy and comprehensive review of affected systems, including performing data mining, to identify the specific individuals and the types of information that may have been compromised. This process was completed on May 24, 2024. On May 28, 2024, Highland Health Systems engaged a third-party notice vendor to assist with the mailings, call center, and provide identity theft protection services. Thereafter, Highland Health Systems worked to verify the information and addresses for mailing.

2. Number of Idaho Residents Notified.

A total of 9 residents of Idaho were potentially affected by this security incident. These individuals are either current or former employees or patients of Highland Health System. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. What Information Was Involved?

The information impacted varied for each individual but included a combination of: Date of Birth, Social Security Number, Account Number, Payment Card Number, Payment Card PIN, Email Address and Password, Medical Information and Health Insurance Information; Tax ID; Routing Number; and Driver's License or State ID.

4. Steps taken in response to the Incident.

Since the discovery of the incident, Highland Health Systems moved quickly to investigate, respond, and confirm the security of their systems. Specifically, Highland Health Systems engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, Highland Health Systems took the following steps, including, but not limited to: disconnected all access to our network; changed administrative credentials; restored operations in a safe and secure mode, implemented security monitoring software, adopted new encryption technologies, deployed additional NIST-compliant technical safeguards, revised policies and procedures, retrained workforce members, and took steps and will continue to take steps to mitigate the risk of future harm.

Data privacy and security is among Highland Health Systems' highest priorities, and they are committed to doing everything we can to protect the privacy and security of the personal information in their care. Although Highland Health Systems is not aware of any evidence of misuse of personal information, Highland Health Systems extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

WILSON ELSER

5. Contact Information

If you have any questions or need additional information, please do not hesitate to contact Joseph Fusz at Joseph.Fusz@wilsonelser.com or 312-821-6141.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph Fusz

Enclosures: *Sample Notification Letter*

WILSON ELSER

EXHIBIT A

HIGHLAND HEALTH SYSTEMS
PSYCHIATRY · PRIMARY CARE · PHARMACY

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/highland

June 13, 2024

Notice of Data Breach

Dear <<Full Name>>,

Highland Health Systems is writing to inform you of a recent data incident (the "Incident") that may have involved some of your personal information. This letter contains details about the Incident, steps we have taken to remediate the Incident, and steps you can take to protect your personal information.

What Happened?

On July 3, 2023, Highland Health Systems detected unusual activity on our network. Upon discovery of this incident, Highland Health Systems immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. During the forensic investigation, Highland Health Systems found evidence that some of our files were accessed by an unauthorized actor.

Based on these findings, Highland Health Systems began a lengthy and comprehensive review of affected systems, including performing data mining, to identify the specific individuals and the types of information that may have been compromised. This process was completed on May 24, 2024. On May 28, 2024, Highland Health Systems engaged a third-party notice vendor to assist with the mailings, call center, and provide identity theft protection services. Thereafter, Highland Health Systems worked to verify the information and addresses for mailing.

What Information Was Involved?

Based on the investigation, the following information related to you may have been subject to unauthorized access: <<Variable Text 1>>.

We take our data responsibilities and protection of your data very seriously and we are sorry for any worry and inconvenience this news will cause. As of this writing, we have not received any reports of related identity theft since the date of the incident (July 3, 2023, to present). We would like to reassure you that we have taken all efforts possible to mitigate any further exposure of your personal information and we are committed to supporting you.

What We Are Doing

Data privacy and security are among Highland Health System's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, Highland Health Systems moved quickly to investigate, respond, and confirm the security of our systems. Specifically, we engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to

determine the nature and scope of the Incident. Additionally, Highland Health Systems took the following steps, including, but not limited to: disconnected all access to our network; changed administrative credentials; restored operations in a safe and secure mode, implemented security monitoring software, adopted new encryption technologies, deployed additional NIST-compliant technical safeguards, revised policies and procedures, retrained workforce members, and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with <<12 24>> months of complimentary credit monitoring and identity theft restoration services through IDX. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-901-3768, going to https://response.idx.us/highland, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 am to 8:00 pm Central. Please note the deadline to enroll is September 13, 2024.

For More Information

Highland Health Systems recognizes that you may have questions not addressed in this letter. Should you have any additional questions representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident. Please do not hesitate to call 1-888-901-3768 (toll free) during the hours of 8:00 am to 8:00 pm Central, Monday through Friday (excluding U.S. national holidays).

We sincerely regret any inconvenience or concern that this matter may cause, and we remain dedicated to ensuring the privacy and security of all information within our control.

Sincerely,
Highland Health Systems

Name
Title

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-349-9960	1-888-397-3742	1-888-909-8872
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 agencies 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 violators. 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 at 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, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, this incident involves 4 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described

above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).