LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

March 16, 2020

VIA E-MAIL
Attorney General Wayne Stenehjem
Office of the Attorney General
500 East Boulevard Ave., Dept. 125
Bismark, ND 58505
E-Mail: ndag@nd.gov

Re: Notification of Data Security Incident

Dear Attorney General Stenehjem:

We represent Avalon Health Care Management, Inc. ("Avalon") in connection with a data security incident which is described in greater detail below. Avalon takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

On July 9, 2019, Avalon became aware of suspicious activity within its email system. Upon making this discovery, Avalon immediately took steps to secure its email system and investigate the activity. As part of the investigation, Avalon engaged an independent digital forensics expert to determine what happened and whether any personal information had been accessed without authorization. On August 5, 2019, Avalon learned that the email account of one of its employees may have been accessed without authorization. Upon completion of the forensic investigation, Avalon engaged a document review vendor to search the contents of the impacted email account to identify the individuals whose personal information may have been contained within the account. On December 16, 2019, Avalon learned that the personal information of some of its patients and employees was contained within the account. Avalon then conducted a thorough review of the information that may have been affected and completed a detailed investigation to identify those individuals whose information was potentially impacted and determine their place of residence. Based upon this analysis, on January 27, 2020, Avalon determined that the names and Social Security numbers of three (3) North Dakota residents and the name, Social Security number, and date of birth of one (1) additional North Dakota resident were

contained within the impacted email account and may have been exposed as a result of this incident.

2. Number of North Dakota residents affected.

Avalon notified the four (4) North Dakota residents of this data security incident via first class U.S. mail on March 16, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps taken relating to the incident.

Avalon has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to enhance the security of its digital environment. Avalon also notified the three major consumer reporting agencies of the incident. Furthermore, while Avalon is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Avalon is also providing twelve (12) months of complimentary identity theft protection services to each letter recipient through Experian. Those services include twelve (12) months of triple bureau credit monitoring, an insurance reimbursement policy, and fully managed identity theft recovery services at no cost to the letter recipients.

4. Contact information.

Avalon 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 (214) 722-7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Respectfully,

/s/ Lindsay B. Nickle

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LMN:arb

Encl.: Sample Consumer Notification Letter

AVALON HEALTH CARE MANAGEMENT

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notification of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident that may have involved some of your personal information. Avalon Health Care Management, Inc. ("Avalon") takes the privacy and security of your information very seriously. This is why we are contacting you, offering you complimentary identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? On July 9, 2019, we became aware of suspicious activity within our email system. Upon making this discovery, we immediately took steps to secure our email system and investigate the activity. As part of the investigation, we engaged an independent digital forensics expert to determine what happened and whether any personal information had been accessed without authorization. On August 5, 2019, we learned that the email account of one of our employees may have been accessed without authorization. Upon completion of the forensic investigation, we engaged a document review vendor to search the contents of the impacted email account to identify the individuals whose personal information may have been contained within the account. On December 16, 2019, we learned that the personal information of some of our patients and employees was contained within the account. We then conducted a thorough review of the information that may have been affected, and on January 27, 2020, we completed a detailed investigation to identify those individuals whose information was potentially impacted and find contact information for those people.

What Information Was Involved? Based on our investigation, the information may include your <<b2b_text_3 (Impacted Data)>>.

What We Are Doing. As soon as we discovered the incident, we took the steps discussed above. In addition, we have taken affirmative action to minimize the likelihood of a similar incident occurring in the future. This includes working with leading cybersecurity experts to enhance the security of our digital environment and reporting the incident to the three major consumer reporting agencies. We are also providing you with information about steps that you can take to help protect your personal information. As an added precaution, we are offering you a complimentary twelve (12) month membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also refer to www.ExperianIDWorks.com/restoration for additional information on how to further protect your personal information. In addition, while we do not believe anyone's information has been misused as a result of this incident, as a precautionary measure to safeguard your information, we encourage you to activate the identity monitoring services being offered at no charge to you by completing the following three easy steps:

1. ENROLL by: **<<b2b_text_1 (Date)>>** (Your code will not work after this date.);
2. Visit the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**; and
3. PROVIDE the **Activation Code:** **<<Member ID>>**.

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **<<b2b_text_2 (Engagement #)>>** as proof of eligibility for the identity restoration services by Experian. Additional information describing the offered services is included with this letter.

For More Information: We remain committed to protecting your personal information and apologize for any worry or inconvenience this may cause you. If you have any questions regarding the incident, please contact Kroll's dedicated call center at 1-???-???-????, Monday through Friday, from 7:00 a.m. to 4:30 p.m. Mountain Time. In addition, as noted above, if you have any questions regarding Experian IdentityWorks Credit 3B, please contact Experian's customer care team at 877-288-8057.

Sincerely,

Fred Shepherd
Vice President of IT | Avalon Health Care Management, Inc.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit or call 877-288-8057 to register with the activation code above.

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of the following states can obtain more information from their Attorney General using the contact information below.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.