LEWIS BRISBOIS BISGAARD & SMITH LLP

Christopher E. Ballod, CIPP/US, CIPP/E
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Christopher.Ballod@lewisbrisbois.com
Direct: 215.977.4077

March 2, 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 the Otis R. Bowen Center for Human Services ("Bowen Center"), which is headquartered in Pierceton, Indiana, regarding a data security incident described in greater detail below. Bowen Center takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

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

Following a search by a document review vendor to identify individuals whose personal information may have been contained within two employee email accounts, on January 28, 2020, Bowen Center learned that the personal information of some of its patients and employees that was contained within those accounts was potentially exposed to an unauthorized user. This discovery was made during the course of an ongoing independent digital forensic investigation. Bowen Center conducted a thorough review of the information that may have been affected and completed its investigation to identify those individuals whose information was potentially impacted and determine their places of residence. Based upon that analysis, Bowen Center learned that the name and limited medical information of two (2) North Dakota residents were potentially impacted by this incident.

2. Number of North Dakota residents affected.

Bowen Center notified the two (2) North Dakota residents of this data security incident via first class U.S. mail on March 2, 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.

Bowen Center has taken steps in response to this incident in an effort to prevent similar incidents from occurring in the future. Those steps include working with leading cybersecurity experts to enhance the security of its digital environment and reporting this incident to the three major consumer reporting agencies. Furthermore, while the Bowen Center is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Bowen Center is also providing twelve (12) months of complimentary identity monitoring services to each letter recipient through Kroll. Those services include free Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

4. Contact information.

Bowen Center 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 (215) 901-6670 or via email at Christopher.Ballod@LewisBrisbois.com.

Please contact me should you have any questions.

Respectfully,

/s/ Christopher E. Ballod

Christopher E. Ballod, CIPP/US, CIPP/E of
LEWIS BRISBOIS BISGAARD & SMITH LLP

CEB:arb

Encl.: Sample Consumer Notification Letter

BOWEN CENTER

<<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. Otis R. Bowen Center for Human Services ("Bowen Center") 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 January 28, 2020, we learned that the personal information of some of our patients and employees contained in two employee email accounts was potentially exposed to an unauthorized user. This discovery was made during the course of an ongoing independent digital forensics investigation. We conducted a thorough review of the information that may have been affected and completed our investigation to identify those individuals whose information was potentially impacted. While we are unaware of any evidence indicating that anyone's information has been misused as a result of this incident, we are providing this letter to you to inform you of the incident and provide steps you can take to further protect your personal information.

What Information Was Involved? Based upon our investigation, the information may include your <<b2b_text_1 (Impacted Data)>>.

What We Are Doing. As soon as we discovered the incident, we completed 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. 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 complimentary identity monitoring services through Kroll for twelve months. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your free identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. Also, 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.

Visit **https://[IDMonitoringURL]** to activate and take advantage of your identity monitoring services.
*You have until **[Date]** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

For More Information: We remain dedicated to safeguarding your personal information and apologize for any worry or inconvenience this may cause you. If you have any questions, please contact Kroll's dedicated call center at 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

Andrew Grimm
Security Officer | Otis R. Bowen Center for Human Services

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL 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	1-877-322-8228	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 Attorneys 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.

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.

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.