LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
One PPG Place
28th Floor
Pittsburgh, PA 15222
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

March 15, 2022

VIA EMAIL
Attorney General Thomas J. Miller
Office of the Attorney General
Consumer Protection Division
Security Breach Notifications
1305 E Walnut Street
Des Moines, IA 50319-0106
E-Mail: consumer@ag.iowa.gov

Re: **Supplement to** Notice of Data Security Incident

Dear Attorney General Miller:

We represent Comprehensive Health Services ("CHS"), a subsidiary of Acuity International, a provider of professional services, specialized consulting, engineering, medical, and environmental solutions, and large-scale program management services for the U.S. government and commercial clients in the national defense, healthcare, international diplomacy, and homeland security markets. Acuity International is headquartered in Reston, Virginia with personnel in 30 countries across five continents. This letter is being sent pursuant to Iowa Code §§ 715C.1-2, because the personal information of Iowa residents may have been affected by a recent data security incident. This letter is being sent to supplement the notice provided on February 15, 2022, because an additional 7 Iowa residents were notified on February 14, 2022. In total, the personal information of 521 Iowa residents may have been affected by this incident. The incident may have included unauthorized access to personal information such as names and Social Security numbers.

On September 30, 2020, CHS detected unusual activity within its digital environment following discovery of multiple fraudulent wire transfers. Upon discovering this activity, CHS immediately engaged a team of cybersecurity experts to secure the digital environment and conduct a forensic investigation to determine the method of initial compromise and access, the scope of the incident, what systems were impacted and whether any personal information may have been accessed or exfiltrated as a result of the incident. Following review and analysis of the information impacted by the incident, and as a result of the investigation, CHS determined on November 3, 2021, that personal information of a limited number of individuals employed by one of its customers may have been accessed or acquired by a malicious actor.

On January 20, 2022, February 15, 2022, and March 14, 2022, CHS notified the affected Iowa residents via the attached sample letter and is offering twelve or twenty four (24) months of credit monitoring and identity protection services through Epiq depending on its contractual obligation. CHS has also taken measures to enhance the security of its network to minimize the likelihood that an event like this might occur again in the future.

Please contact me at Lauren.Godfrey@lewisbrisbois.com should you have any questions.

Sincerely,

Lauren D. Godfrey

Lauren Godfrey, CIPP (US/E) of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

Comprehensive Health Services
Workforce Health Solutions Made Easy

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

Comprehensive Health Services ("CHS") was the target of a cyber intrusion that may have involved your personal information. CHS takes the privacy and security of your information very seriously, and while there is no evidence that your personal information has been used inappropriately, we are informing you of the incident and offering you complimentary credit monitoring and identity protection services. CHS provides occupational health services for your current or former employer, <<AGENCY/COMPANY >>. Our records indicate that you attended one or more physical exams scheduled by CHS.

What Happened: CHS detected suspicious activity within its network. We immediately launched an investigation and engaged cybersecurity experts to assist in our response to the incident. Furthermore, we reported the incident to law enforcement, including the Federal Bureau of Investigation ("FBI"), in hopes of holding the perpetrator(s) accountable. On November 3, 2021, as part of the investigation into the cyber intrusion, CHS learned that some personal information of current and former employees of the <<AGENCY/COMPANY >> was in certain invoicing files pre-dating 2019. These invoicing files are the ones that may have been accessed or acquired without authorization. Once discovered, CHS worked diligently to confirm the scope of those affected and remediate the incident for all impacted individuals.

What Information Was Involved: Your <<Impacted Information>> may have been accessed or acquired without authorization during the incident.

What We Are Doing: In addition to engaging with law enforcement, the Company implemented additional corrective actions as recommended by the forensic review team during its investigation. We have invested in enhanced network security measures, including: 1) purchasing a new suite of endpoint detection and response tools, and installing this software on all servers and endpoints on the network enterprise; 2) replacing our previous threat detection and monitoring surveillance vendor; 3) adding capabilities for extended detection and response to future attempted network intrusions; and 4) conducting network penetration testing.

To alleviate concerns over possible identity theft as a result of this incident, and to restore confidence following this incident, we are offering you complimentary identity protection services through **Equifax,** a leader in risk mitigation and response. This service includes 24 months of credit monitoring, dark web monitoring, a $1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery service.

As noted above, to date there is no evidence your information has been misused. However, we encourage you to take full advantage of this service offering.

What You Can Do: We encourage you to enroll in the complimentary services offered by going to **www.equifax.com/activate** and using the enrollment code <<ENROLLMENT CODE>> to initiate those services. Please note that the deadline to enroll is <<Enrollment DEADLINE>>.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call **800-741-0381** between **9 am to 9 pm Eastern**.

8600 Astronaut Blvd
Cape Canaveral, FL 32920
(321)783-2720

Please also note that neither CHS nor <<AGENCY/COMPANY >> **will contact you to confirm any personally identifiable information. If you are contacted by anyone purporting to represent CHS or** <<AGENCY/COMPANY >> **and asking you for your information, do not provide it.**

We remain dedicated to protecting your personal information and deeply regret any concern or inconvenience this may cause you.

Sincerely,

Comprehensive Health Services

8600 Astronaut Blvd
Cape Canaveral, FL 32920
(321)783-2720

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 by reviewing 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 also should 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 (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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.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: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. 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 fraud alerts, security freezes, and 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.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

8600 Astronaut Blvd
Cape Canaveral, FL 32920
(321)783-2720