K&L GATES

October 18, 2023

Gina L. Bertolini
gina.bertolini@klgates.com

T +1 919 466 1108
F +1 919 516 2008

**VIA EMAIL (consumer@ag.iowa.gov)**

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

**Re: Notice of Data Security Incident – BHI Energy | Specialty Services LLC**

To Whom It May Concern:

Please be advised that we are legal counsel to BHI Energy | Specialty Services LLC ("BHI"). We write regarding a recent data security incident at BHI. For over 40 years, BHI Energy ("BHI") has provided support, including specialty services and staffing solutions, to the nuclear, fossil, hydro, wind, and solar generation power markets. BHI is located at 97 Libbey Industrial Parkway, 4th Floor, Weymouth, Massachusetts 02189.

On June 29, 2023, BHI's information technology team initially identified evidence that data within its network had been encrypted. BHI immediately initiated business continuity and security response efforts, taking steps to isolate the involved systems to stop propagation of the incident, while ensuring that it could continue its business operations with only minor disruption as it responded to, investigated, and recovered from the incident. As part of that process, also on June 29, 2023, BHI retained outside counsel and, through counsel, retained an outside third party cybersecurity firm to investigate the incident.

The cybersecurity firm determined that the threat actor (TA), operating under the name "Akira," gained initial access to BHI's network on May 30, 2023. The TA's initial access was achieved by using a previously compromised user account of a third-party contractor. Using that third-party contractor's account, the TA reached the internal BHI network through a VPN connection. In the week following initial access, the TA used the same compromised account to perform reconnaissance of the internal network. On June 16, 2023, the TA returned to the network and performed further data reconnaissance, and on June 18, 2023, began staging data. The TA ultimately exfiltrated 690 gigabytes of data between June 20, 2023, and June 29, 2023, including a copy of BHI's Active Directory database. On June 29, 2023, having completed exfiltration of the data, the TA deployed the Akira ransomware to a subset of systems within BHI's network. The TA provided a file listing that referenced 767,035 files exfiltrated, totaling 690GB of uncompressed data. The TA created and subsequently deleted these archives on a BHI server.

Immediately upon learning of the incident, BHI brought in an outside forensic consultant operating under the guidance of outside legal counsel, and began taking actions to remove the TA from the network and to recover involved systems. BHI also promptly contacted law enforcement. Because the company's cloud backup solution was not affected, BHI was able to successfully recover data in the systems without needing to obtain a ransomware decryption tool from the TA. After removing the TA from BHI's network, which occurred on or about July 7, 2023, BHI extended its deployment of EDR and antivirus software within the environment; performed an Enterprise Password Reset; decommissioned legacy and unused systems; and implemented multi-factor authentication on its remote access VPN.

Once the cybersecurity firm identified the systems impacted, BHI, with outside counsel's data analytics and forensics team, reviewed and analyzed files impacted by the breach. On or about September 1, 2023, BHI identified that some of the files contained individuals' personal information and, in the ensuing days, BHI was able to identify the specific data disclosed, which consisted of first, middle, and last name, address, date of birth, and Social Security number, and potentially health information. On October 4, 2023, BHI initially confirmed the identities and addresses of the eight hundred and ninety-six (896) affected Iowa residents. BHI sent written notice to these residents today, October 18, 2023. The notice provided to those residents is also enclosed.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

Gina L. Bertolini

Return Mail Processing
PO Box 999
Suwanee, GA 30024

416 1 91266 **********AUTO**ALL FOR AADC 870
SAMPLE A. SAMPLE - PII
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

October 18, 2023

**Notice of Data Security Incident**

Dear Sample A. Sample:

We are writing to inform you of a data security incident at BHI that may have exposed some of your personal information. BHI takes the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

**What Happened?**

On or about June 29, 2023, BHI's IT and Security teams determined that certain systems hosted on the BHI network were subject to unauthorized access. Upon discovery, BHI promptly investigated the incident and notified federal and local law enforcement, removed the threat, and secured BHI's computing environment.

After a thorough investigation, on September 1, 2023, BHI learned that certain BHI business records stored in BHI's network, including some records that contained personally identifiable information ("PII"), were subject to unauthorized access. On October 4, 2023, BHI identified the individuals whose PII was involved in the event.

**What Information Was Involved?**

Through ongoing investigation, BHI determined that your personal information was included in the files affected by this incident.

The information that may have been included are your first, middle, and last name, address, date of birth, and Social Security number, and potentially health information.

**What We Are Doing**

Upon discovering the incident, and to mitigate any potential harm, BHI immediately took action to contain the incident and to secure and restore the involved systems. We then retained a leading third-party forensic consulting firm to investigate the nature and scope of the incident and to assist us in putting additional security measures in place. We notified federal and local law enforcement authorities, and we are notifying state and federal agencies, as required by state privacy laws.

We are further offering a complimentary 24-month membership to Experian's® IdentityWorks℠ at no cost to you. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **January 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus
- Provide your **activation code**: **ABCDEFGHI**

**What You Can Do**

In addition to activating identity monitoring services, please review the "Recommended Steps to Help Protect Your Information" section included with this letter, which describes additional steps you can take to protect yourself, including recommendations by the Federal Trade Commission regarding how to place a fraud alert or a security freeze on your credit file.

**For More Information**

We understand how important this matter is to you. We value our employees and customers and are committed to protecting personal information. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 844-262-8351, Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Please be prepared to provide engagement number B103348 when you call.

Sincerely,

Mark Laverty
Information Officer
BHI Energy

**Recommended Steps to Help Protect your Information**

**CREDIT MONITORING**

**ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:**

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

You can contact Experian **immediately** regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 844-262-8351. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

**CREDIT REPORTS**

We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**FRAUD ALERTS**

Place fraud alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

**CREDIT BUREAUS**

| Equifax Fraud Reporting | Experian Fraud Reporting | TransUnion Fraud Reporting |
|---|---|---|
| 1-866-349-5191 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5069 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | www.transunion.com |

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**SECURITY FREEZE**

By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**ADDITIONAL INFORMATION**

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.

New Mexico Residents: You 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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

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: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.