June 30, 2023

Via E-Mail

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

To Whom It May Concern:

I write on behalf of Genesis Energy, L.P. (the "Company") to provide notice of a security incident potentially affecting four New Hampshire residents.

Genesis received an alert on June 1, 2023, from one of its security contactors of a potential cyberattack on third-party software used to host Genesis' file transfer site. In response, the Company's IT Team disabled access to the site and began investigating. Based upon the security alert and the Company's initial investigation, the Company determined that the cyberattack had exploited a previously unknown vulnerability in the third-party software used to host the file transfer site. Shortly thereafter, the software maker released a patch to repair the software, which the Company immediately installed. Genesis has since learned that it is just one of many companies globally victimized by this cyberattack which exploits the same vulnerability in the MOVEit software, provided to Genesis by Progress Software. Based on information Genesis has received about the incident, the Company believes that the identity of the unauthorized third party(ies) is "Lace Tempest", part of the "cl0p" ransomware group.

The Company's investigation has determined that the unauthorized third party copied files from the site that contained the information of current or former Genesis employees, and dependents of current employees who are enrolled in a Genesis health plan. These files contained the personal information of four New Hampshire residents, including their .

We sent the attached notification to all potentially affected New Hampshire residents. Out of an abundance of caution, we offered of identity theft protection services at no cost to potentially affected individuals.

Although the cyberattack was directed towards the third-party software used to host the Company's file transfer site rather than the Company itself, Genesis has undertaken a thorough investigation into this incident, and has taken steps to prevent a recurrence, including promptly patching the vulnerability and reviewing relevant security protocols to identify ways to enhance information security. Genesis has also contacted law enforcement regarding this incident and will cooperate in their investigations.

If you have any questions concerning this matter, please do not hesitate to contact our counsel at .

Very truly yours,

Robert Deere
Chief Administrative Officer
Genesis Energy, L.P.

genesisenergy

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[NAME]
[ADDRESS]
[CITY], [STATE] [ZIP]

June 30, 2023

Dear [Name]:

Genesis Energy, L.P. ("Genesis" or the "Company") values its employees, both current and former, and is committed to protecting your personal information. Unfortunately, I am writing to inform you of a cyberattack on the Company's file transfer site and to share with you the steps that Genesis is taking to address it. Genesis currently has no reason to believe that your personal information has been misused as a result of this incident. You are being notified as a precautionary step and because it is important to be transparent with you about any incident involving your personal information.

Genesis received an alert on June 1, 2023, from one of its security contactors of a potential cyberattack on third-party software used to host Genesis' file transfer site. In response, the Company's IT Team disabled access to the site and began investigating. Based upon the security alert and the Company's initial investigation, the Company determined that the cyberattack had exploited a previously unknown vulnerability in the third-party software used to host the file transfer site. Shortly thereafter, the software maker released a patch to repair the software, which the Company immediately installed. Genesis has since learned that it is just one of many companies globally victimized by this cyberattack which exploits the same vulnerability in the third-party software provider's software.

The Company's investigation has determined that the unauthorized third party copied files from the site that contained your personal information, . If you have a spouse or dependents who were enrolled in a Genesis health plan while you were employed by the Company, their personal information may have been impacted by this incident. In that event, your spouse and/or dependent(s) will each receive their own notice letter.

.

Out of an abundance of caution, the Company has contracted with NortonLifelock to provide all impacted individuals with of identity theft protection services, at no cost to you, your spouse or dependents. Membership in NortonLifeLock's "LifeLock Defender™ Preferred" product provides credit monitoring, fraud detection tools, dark web monitoring, identity restoration services and other benefits. To activate your membership in Norton LifeLock Defender™ Preferred, complete the following steps.

4. A popup will appear. Enter your Member ID and click “APPLY”. This is a unique, one-time code to be used by the enrollee. Your Member ID is:
5. Next, you will be prompted to set up an account. If you already have an account with Norton, you will be prompted to provide your existing account credentials.
6. After your information has been entered, you will receive confirmation of your activated membership at the email address you have provided.
7. If you plan to add minor children, you must have the social security number and birth date for each minor to be enrolled. You can also add minor dependents at a later time after activation of your membership by clicking on Manage My Subscriptions. Minor children will be enrolled into the Norton LifeLock Junior™ program.

If you prefer to activate your membership by phone or have any difficulty activating your membership, please call: . You can also call this toll-free phone number if you have questions about the identify theft protection benefits being provided. The enrollment deadline for LifeLock Defender™ Preferred is

In addition to the offer of LifeLock Defender™ Preferred, included with this letter is additional information on steps you can take to protect the security of your personal information. I urge you to review this information carefully.

Please be assured that the Company takes seriously both the security of your personal information and this incident. Although the cyberattack was directed towards the third-party software used to host the Company’s file transfer site rather than the Company itself, in response to this incident, Genesis promptly patched the vulnerability and took other steps to prevent a recurrence. The Company has also notified law enforcement of this incident and will cooperate in any investigation.

The Company regrets this incident and any inconvenience it may cause you. Should you have any questions or concerns regarding this incident, please do not hesitate to contact our call center at [Number] between 8 A.M. and 6 P.M (CST), Monday through Friday.

Sincerely,

Bob Deere
Chief Administrative Officer
Genesis Energy, L.P.

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. **Enroll in LifeLock Defender™ Preferred.** You must personally enroll in this service for it to be effective. The e-mail notification contains instructions and information on how to activate your membership. Membership in LifeLock Defender™ Preferred includes:

- Primary Identity Alert System[1]
- 24/7 Live Member Support
- Dark Web Monitoring
- Norton™ Security Deluxe (90 Day Free Subscription)[2]
- Stolen Funds Reimbursement up to $25,000, Personal Expense Compensation up to $25,000, and Coverage for Lawyers and Experts up to $1 million[3]
- U.S.-based Identity Restoration Team
- Annual Three-Bureau Credit Reports & Credit Scores
- Three-Bureau Credit Monitoring[4]
- USPS Address Change Verification Notifications
- Fictitious Identity Monitoring
- Credit, Checking and Savings Account Activity Alerts

If you have questions about the identity theft protection benefits offered, please contact NortonLifeLock at .

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled to one free copy of your credit report from each of the three national credit bureaus every 12 months. Until December 31, 2023, however, you are entitled to a free copy of your credit report from each of the three national credit bureaus once a week. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. Errors in information in your credit report may be a sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your credit report, whether or not due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

---

[1] LifeLock does not monitor all transactions at all businesses.

[2] Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

[3] Reimbursement and Expense Compensation, each with limits of up to $25,000 for Defender Choice. And up to $1 million for coverage for lawyers and experts if needed, for all plans. Benefits provided by Master Policy issued by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

[4] If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from NortonLifeLock, contact NortonLifeLock's live member support for more information and assistance. You should consider changing your username, passwords, security questions, and security answers to any of your online accounts where your payment card information is stored as well as for financial institutions. If you notice suspicious activity on an account statement, report it to your credit card company or other service provider and consider closing the account. You should also consider reporting such activity to your local police department, your state's attorney general, and the Federal Trade Commission.

5. You have the right to place a "security freeze" on your credit report. A security freeze will prohibit a consumer reporting agency from releasing information in your credit file without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Please understand that placing a security freeze on your credit file may delay, interfere with, or prevent the timely approval of any subsequent request or application you make for a new loan, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

To place a security freeze on your credit file, contact the three nationwide credit bureaus, listed below. You will need to provide appropriate proof of your identity to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. There is no charge to place a credit freeze.

The contact information for all three credit bureaus is as follows:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

6. Consider placing a fraud alert with one of the three nationwide credit bureaus. You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

7. Additional Information. You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; http://www.ftc.gov/idtheft/; (877) IDTHEFT (438-4338).

If you live in Maryland, please read the additional notice below that applies to you:
You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

If you live in Massachusetts, please read the additional notice below that applies to you:
Massachusetts law gives you right to report this incident to the police in the county where you reside and to receive a police incident report within 24 hours of filing.

If you live in New Mexico, please read the additional notice below that applies to you:
Please visit the following link to review a summary of your major rights under the federal Fair Credit Reporting Act (FCRA):

https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

If you live in New York, please read the additional notice below that applies to you:
You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
www.ag.ny.gov/

If you live in North Carolina, please read the additional notice below that applies to you:
You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226 (within North Carolina)
1-919-716-6000 (outside of North Carolina)
www.ncdoj.gov

If you live in Wyoming, please read the additional notice below that applies to you:
Law enforcement has not requested that we delay notifying you.