JacksonLewis

Jackson Lewis P.C.
200 Connell Drive., Suite 2000
Berkeley Heights, NJ 07922
(908) 795-5200 Main
(908) 464-2614 Fax
www.jacksonlewis.com

Mary Costigan, Esq.
Direct: (908) 795-5135
mary.costigan@jacksonlewis.com

November 2, 2021

VIA CERTIFIED MAIL
Office of the Attorney General
Department of Justice
Consumer Protection Bureau
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[1]

Dear Sir or Madam:

Please be advised that on September 14, 2021, our client, Mowery Clinic ("Mowery"), learned that personal and/or protected health information of three (3) New Hampshire residents may have been subject to unauthorized access or acquisition as the result of a cyberattack (the "Incident"). Mowery is a medical clinic located at 737 E. Crawford St., Salina, KS.

Based on the underlying investigation, it appears the Incident occurred on or around September 8, 2021. The data elements involved may have included name, address, birth date, medical information such as office notes and diagnostic reports and, in limited circumstances, a Social Security Number.

Immediately upon learning about the Incident, Mowery commenced an investigation to determine the scope of the Incident and identify those potentially affected. This included Mowery working with its information technology team and third-party forensic experts in an effort to ensure the Incident did not result in any additional exposure to personal or health information, and to determine what information may have been accessed or acquired. The investigation determined that the unauthorized actor did not access Mowery's electronic health record ("EHR") database but may have gained access to certain Mowery files containing personal

[1] Please note that by providing this letter Mowery is not agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

or protected health information. The investigation was unable to determine what information contained in the files was accessed or acquired as a result of this Incident.

While it is believed the number of affected individuals is limited to a small subset of Mowery's patients and employees, Mowery has chosen to notify all patients out of an abundance of caution. In light of this Incident, Mowery plans to begin notifying individuals in the next several days. A draft copy of the notification that will be sent is enclosed with this letter.

As set forth in the enclosed letter, Mowery has taken steps to protect the security of the personal and protected health information of all patients. In addition to continuing to monitor this situation, Mowery is reviewing its current privacy and data security policies and procedures to minimize the chances of this happening again. Should Mowery become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS, P.C.

/s/ Mary Costigan
mary.costigan@jacksonlewis.com
200 Connell Drive, Suite 2000
Berkeley Heights, NJ 07922
PH: (908) 795-5135
FAX: (908) 464-2614

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

As a current or former patient of Mowery Clinic in Salina, Kansas, we are notifying you of a data incident that may have involved your protected health information and personal information.

What Happened

On September 14, 2021, Mowery Clinic learned it was the victim of a sophisticated cybersecurity attack. We promptly took steps to secure our network and engaged a third-party cybersecurity firm to conduct a forensic investigation into the cause and scope of the attack. The investigation determined that an unauthorized individual had gained access to our network. The individual did not access Mowery Clinic's electronic medical records application; however, the individual deployed malware and accessed or acquired certain documents in our systems that contain patient information.

What Information Was Involved

This information may have included the following: name, address, date of birth, medical information such as office notes and diagnostic reports and, in limited circumstances, a Social Security Number. At this time, we have no indication that any of your information has been used to commit identity theft or fraud.

What We Are Doing

Mowery Clinic endeavors to protect the privacy and security of patient information. We are working diligently to determine how this incident happened and taking appropriate measures to prevent a similar situation in the future.

What You Can Do

As with any data incident, we recommend that you remain vigilant and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. We have included a list of suggested measures at the end of this letter.

For More Information

We apologize for any concern this incident may cause you. Please call [TFN] or go to https://response.idx.us/customending for assistance or for any additional questions you may have.

Sincerely,

Jennifer VonLintel
Administrator

Mowery Clinic

(Enclosure)

Recommended Steps to Help Protect Your Information

1. Place a 90-day fraud alert on your credit file. An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the credit cannot verify that you have authorized this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

   Experian: 1-888-397-3742; www.experian.com
   TransUnion: 1-800-680-7289; www.transunion.com
   Equifax: 1-800-525-6285; www.equifax.com

2. Place a security freeze on your credit. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also accessed through each of the credit reporting companies and there is no charge.
   To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

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

   In order to request a security freeze, you may need to provide the following information:

   1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
   2. Social Security Number;
   3. Date of birth;
   4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
   5. Proof of current address such as a current utility bill or telephone bill;
   6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
   7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

3. Order your free annual credit reports. Visit www.annualcreditreport.com or call 877-322-8228 to obtain a free annual credit report. Once you receive your credit report, review it for discrepancies, identify accounts you did not open or inquiries from creditors that you did not authorize, and verify all information is correct. If you have questions, or notice any incorrect information, contact the credit reporting company.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

4. Use tools from credit providers and monitor your statements. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on your credit cards and bank accounts for notice of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. We also recommend that you review the statements you receive from your healthcare provider and health insurer. If you see any charges for services that you did not receive, please call the provider or insurer immediately.

5. Report suspected identity theft. 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, the Attorney General, or the Federal Trade Commission.

6. Your Rights Under the Fair Credit Reporting Act: The Fair Credit Reporting Act (FCRA) establishes procedures to correct mistakes on your credit record and requires that your record be made available only for certain legitimate business needs. Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report. Your major rights under the FCRA are summarized below.

    - You must be told if information in your file has been used against you.
    - You have the right to know what is in your file.
    - You have the right to ask for a credit score.
    - You have the right to dispute incomplete or inaccurate information.

- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

To protect your rights under the law, contact both the credit bureau and the information provider. For additional information, visit www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

7. For information on Medical Identity Theft, please see the Federal Trade Commission (FTC) brochure, Medical Identity Theft (consumer.ftc.gov/articles/0171-medical-identity-theft.

8. To contact the FTC, or for additional information on identity theft, please call or contact the FTC at 877-436-4338, TTY 866-653-4261.
www.ftc.gov/idtheft.
Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

9. Residents of Maryland: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (410) 576-6491, and http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

   Residents of New York: You may obtain additional information from the New York State Police, 1220 Washington Avenue, Building 22, Albany, NY 12226-2252 or https://www.troopers.ny.gov/ and the Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Suite 640, Albany, NY 12231, Phone: (800) 697-1220 and https://www.dos.ny.gov/consumerprotection/.

   Residents of North Carolina: you may obtain information about preventing identity theft from the following source: Office of the Attorney General, 0001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, and www.ncdoj.gov/Home/ContactNCDOJ.aspx.

   Residents of Oregon: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; (503) 378-4400 and http://www.doj.state.or.us/Pages/Index.aspx.