Centrelake Medical Group, Inc. ("Centrelake") engages Data Media Associates, LLC ("DMA") to provide printing, mailing, and other healthcare billing fulfillment services. DMA may mail patient billing statements, paper insurance claims, or other letters on behalf of Centrelake.

In June of 2023, DMA reported it became aware of an alert issued by the Cybersecurity and Infrastructure Security Agency addressing a critical vulnerability affecting MOVEit Transfer, a managed file transfer solution used widely by businesses and government agencies, including DMA, to securely transfer data. After becoming aware of the alert, DMA indicated it took steps to ensure the security of its MOVEit system and conducted an investigation with the assistance of external cybersecurity specialists to learn more about the scope of any potentially affected data. DMA's reported investigation concluded on June 30, 2023, and revealed that certain data stored within MOVEit may have been acquired without authorization. We encourage you to review DMA's website to learn more about the event and DMA's response: https://www.dma.us/NoticeOfSecurityIncident.htm.

On or around July 28, 2023, DMA notified Centrelake that certain information associated with the organization may have been downloaded by an unauthorized party. This may have included patient statements and health care financing administration claims that DMA produces, prints, and mails on behalf of Centrelake. DMA indicated it has taken remediation measures recommended by the MOVEit software developers and will be evaluating additional safeguards that can be put in place to further enhance the security of the data entrusted to it.

DMA provided notice of this event via written letter to potentially affected individuals associated with Centrelake beginning on September 25, 2023. Although Centrelake has not been made aware of any actual misuse of this information, itis providing information about the event, DMA's response, and steps potentially affected individuals may take to better protect against the possibility of identity theft and fraud, should they feel it is necessary to do so.

The following information may have been involved in DMA's MOVEit event include: first and last name, address, and high-level medical or health insurance information such as would appear on billing statements, invoices, or other claims-related documents. This may include service date(s), service description, insurance name, and/or payment balance information. It would not include substantive payment information, such as financial account numbers. In some instances, the involved data also included health insurance identification numbers, which may be the same as an individual's Social Security number. The relevant information associated with potentially affected individuals is included in the letter DMA provided.

DMA established a toll-free call center to answer questions about the event and to address related concerns. Call center representatives are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time and can be reached at (888) 979-0013. You may also write to Centrelake Medical Group, Inc at 3115 E Guasti Rd, Ontario, CA 91761.

As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, explanations of benefits, and credit reports for unusual activity and to detect errors. Additional resources can be found below in the *Steps You Can Take to Help Protect Your Information.*

Steps You Can Take To Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. Notifications were not delayed by law enforcement.