Notice of Potential Data Compromise

The privacy and security of the personal information we maintain is of the utmost importance to Lamont Hanley & Associates, Inc. ("LH"). We want to inform individuals of a data security incident that has affected our organization, and let you know that we continue to take significant measures to protect individual personal and health information. On June 20, 2023, LH discovered one employee email account was accessed by an unauthorized party via a phishing attempt. Upon detecting the incident, LH commenced an immediate and thorough investigation, contained and secured the email environment, and changed the password to the affected email account.

As part of the investigation, LH engaged external cybersecurity professionals to investigate the extent of the incident and what, if any, sensitive data, including personal and/or health information may have been accessed and/or acquired by the unauthorized party. The investigation did not identify evidence of specific data access or acquisition by an unauthorized party, but could not conclude with one-hundred percent certainty that data within the account was not accessed or acquired by an unauthorized party. Therefore, out of an abundance of caution, we conducted an extensive review of affected email account to determine what data may have been involved. After a thorough forensic investigation and comprehensive manual review of all data within the account, December 29, 2023, we determined the specific personal information present within the account. We immediately worked with our business partners to notify affected individuals of this incident. On February 28, 2024, we identified additional personal information may have been involved. The information involved may include individual name, Social Security Number, date of birth, medical and claim information, health insurance information, individual identification information, and financial account information.

To date, we are not aware of any reports of identity fraud or improper use of individual personal and/or health information as a direct result of this incident. LH is notifying affected individuals via mail about the incident, and including in the communication steps individuals may take to protect the privacy of their personal information.

We remind individuals to remain vigilant in reviewing financial account statements on a regular basis for any fraudulent activity. We also recommend that individuals review the explanation of benefits statements that they receive from their health insurance providers, and follow up on any items not recognized. Please see the "Other Important Information" section below with additional information to help further safeguard your personal data.

We are committed to maintaining the privacy of personal and health information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-833-792-8144. This response line is staffed with professionals familiar with this incident and

knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
1-888-909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.