



Notice of Data Breach

Fort Worth, Texas – February 14, 2025 – Lena Pope Home, Inc. (“Lena Pope”) is writing to inform you of a recent data security incident that may have resulted in the unauthorized access to some individuals’ personal information. While this incident did not significantly impact our ability to continue servicing our clients, this notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of personal information.

What Happened? On January 16, 2025, Lena Pope discovered an employee’s email account had been compromised. Upon discovery of this incident, Lena Pope immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. While the forensic investigation is ongoing, Lena Pope’s preliminary internal investigation found evidence to suggest some of its emails and files may have been accessed by an unauthorized actor. On January 23, 2025, Lena Pope determined that certain personal information may have been included in the impacted email account. Please note that Lena Pope’s electronic medical records (“EMR”) system was not impacted by this incident.

Based on these findings, Lena Pope promptly reviewed the affected emails and files to identify the specific individuals and the types of information that may have been compromised. On February 13, 2025, Lena Pope finalized the list of individuals to notify.

What Information Was Involved? Based on the investigation, the following information related to potentially impacted individuals may have been subject to unauthorized access: first name/initial and last name; telephone number; email address; date of birth; admission date; individual/Medicaid number; health insurance policy number; date and type of service received; household size/income; self-reported reason for counseling; insurance copay/deductible information; and if there is an open child protective services (“CPS”) case. For only a limited number of individuals progress towards treatment goals may have been accessed. The information potentially impacted varies by individual and is applicable only if that information was provided to Lena Pope (not all information was actually provided to Lena Pope for all individuals). **Please note that Social Security Numbers and financial information were not impacted in this incident.**

What We Are Doing? Data privacy and security is among Lena Pope’s highest priorities and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, Lena Pope moved quickly to investigate and respond to the incident, assess the security of its systems, and notified potentially affected individuals. Specifically, Lena Pope internally investigated the incident and engaged a specialized third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. Lena Pope also implemented enhanced technical safeguards, implemented multifactor authentication and GEO IP blocking for Office 365, provided additional security training for staff members, and enhanced data security measures and will continue to enhance the security of our systems. Lena Pope also reviewed all impacted emails and files to identify the potentially affected individuals in preparation for notice. We take the protection and proper use of personal information very seriously.

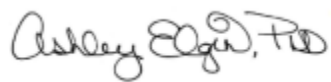
What You Can Do: We encourage you to remain vigilant for the next 12 to 24 months and take steps to protect yourself against identity theft and fraud, including monitoring your accounts and account statements and promptly reporting incidents of suspected identity theft to the relevant institution. We also recommend monitoring your free credit reports for suspicious activity or unauthorized activity. You have the right to obtain

a police report. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a free security freeze and fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to place security freezes and fraud alerts on your credit file and how to further protect against the possibility of information misuse.

For More Information: Representatives are available for 90 days from the date of this letter to you to assist with questions regarding this incident between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding U.S. national holidays. Please call the tollfree help line at 1-833-799-3873 and supply the representative with the unique code listed on this letter.

Lena Pope sincerely regrets that this incident occurred and any inconvenience that it may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

A handwritten signature in cursive script that reads "Ashley Elgin, PhD".

Dr. Ashley Elgin
Chief Executive Officer
Lena Pope Home, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General’s office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and Transunion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374- 0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
Transunion	P.O. Box 1000 Chester, PA 19016- 1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.ny.gov/consumer-protection>; by visiting the New York Attorney General at <https://ag.ny.gov/>

or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.