PO Box 5012
Branchburg NJ 08876

<Date>

0000001

<FIRST NAME> <LAST NAME>
<ADDRESS 2>
<ADDRESS 1>
<CITY>, <STATE> <ZIP CODE>

NOTICE OF DATA BREACH

Dear <first Name> <last Name>,

We at Clayton Properties Group, Inc. (d/b/a Mungo Homes) ("**Mungo**") are writing to inform you about a data-security event involving some of your personal information. We are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll in our offer of free identity-theft-protection services.

What Happened. On or around May 6, 2026, an unauthorized third party used social engineering techniques to register a new multifactor authentication (MFA) device and obtain login credentials, thereby gaining access to a Mungo employee's OneDrive, SharePoint, and email accounts. Upon discovering this activity, Mungo initiated a forensic investigation and determined that between approximately May 6 and May 11, this threat actor downloaded files from these accounts. Further investigation showed that some of the files accessed contained personal information. The specific data elements involved vary by individual and file but may have included one or more of the following data elements: name, social security or individual tax ID numbers, financial account numbers, dates of birth, driver's license, addresses, and medical/prescription or insurance information. On July 1, 2026, the forensic investigation discovered that the aforementioned personal information had been potentially compromised. The investigation found no evidence of any further lateral movement or compromise of any other employee accounts beyond those identified above.

What Information Was Involved. Following our forensic investigation, we have determined that the impacted files contained some of your personal information, which includes your <Data Elements>.

What We Are Doing. Mungo values your privacy and deeply regrets that this incident occurred. We have been working with both internal and external resources to remediate the situation, emphasize compliance with our company's security policies and procedures, and implement security measures designed to prevent a recurrence of similar incidents in the future. We are notifying you so that you are aware of what happened here. We believe it is important to be upfront with everyone involved.

What You Can Do. We encourage you to remain vigilant for any signs of unauthorized financial activity and review the Additional Steps You Can Take guidance on the next page. Additionally, to help protect you from fraud or identity theft, we are offering you a complimentary <**12**>- month membership to <Product>, a credit and identity-theft monitoring service.

To register, please:

- Ensure that you enroll by: <Enroll Date> (Your code will not work after this date.)
- Visit the <Product> website to enroll: <URL>
- Provide your activation code: <Activation Code>

0000001

If you have questions for <Product>, please contact them directly at <Phone Number> by <Date>.

For More Information. Should you have any questions, you can contact us at <Call Center Number>, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Clayton Properties Group

ADDITIONAL STEPS YOU CAN TAKE

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Report Incidents

It is always advisable to remain vigilant against attempts at identity theft or fraud, including by reviewing your free credit reports and account statements closely for signs of suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to the proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact your local police or law enforcement, the Federal Trade Commission ("FTC"), and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. The FTC's contact details are provided below.

Federal Trade Commission Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)
1-877-FTC-HELP (382-4357

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax	P.O. Box 740241 Atlanta, GA 30374	www.equifax.com www.equifax.com/personal/credit-report-services	800-685-1111
Experian	P.O. Box 2002 Allen, TX 75013	www.experian.com www.experian.com/help	888-397-3742
TransUnion	P.O. Box 1000 Chester, PA 19016	www.transunion.com www.transunion.com/credit-help	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You have the option to place a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. You may also obtain information about fraud alerts from the FTC.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill. For more information about requesting a security freeze, you may contact the credit reporting agency at the contact information provided above. You may also obtain information about security freezes from the FTC.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: 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; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights pursuant to the FCRA.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you have the right to file a police report. You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400 for more information about steps you can take to help avoid identity theft.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E Walnut St, Des Moines, IA 50319, 515-281-5926 or 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023 for more information about steps you can take to help avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report and request a security freeze as described above.

For New York residents: You can contact the New York Department of State Division of Consumer Protection, 99 Washington Avenue, Albany, NY 12231, http://www.dos.ny.gov/consumerprotection,1-800-697-1220 or the New York Attorney General, The Capitol, Albany, NY 12224, http://www.ag.ny.gov/,1-800-771-7755 for information about steps you can take to help avoid identity theft.

For New Mexico Residents: You have rights pursuant to the FCRA, as described above. You may have additional rights under the FCRA not summarized here. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by contacting the FTC at the contact information listed above.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226 for information about steps you can take to help avoid identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

For Rhode Island residents: You can contact the Rhode Island Attorney General,150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400. You have the right to obtain a police report and request a security freeze as described above.