Alexandra Belton
abelton@mullen.law
Office: (267) 930-4773
Cell: (215) 805-6437

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 29, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Lyon Management Group, Inc. ("Lyon") located at 4901 Birch St, Newport Beach, CA 92660, and write to notify your office of an incident that may involve certain personal information relating to approximately four (4) Maryland residents. By providing this notice, Lyon does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 15, 2024, Lyon became aware of suspicious activity involving its network and promptly began an investigation into the nature and scope of the suspicious activity. As a result of its investigation, Lyon determined that certain systems were accessed by an unknown actor between March 14, 2024, and March 15, 2024, and that certain files were potentially copied from the environment during that time. Lyon then undertook a thorough review of those files to determine what information was present, to whom it relates, and contact information for those individuals. While these efforts are ongoing, Lyon recently determined the data may include information related to four (4) residents of Maryland. The information that could have been subject to unauthorized access includes name, driver's license number, and Social Security number.

Notice to Maryland Residents

On or about January 29, 2025, Lyon provided written notice of this incident to four (4) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

In response to this incident, Lyon took steps to secure its IT systems and commenced a thorough investigation into the full nature and scope of the incident, including what data may be affected. Further, Lyon notified federal law enforcement. Additionally, Lyon is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Lyon is also providing potentially affected Maryland residents with access to credit monitoring services for twelve (12) months through TransUnion at no cost.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4680.

Very truly yours,

Alexandra Belton of
MULLEN COUGHLIN LLC

AGC/agc
Enclosure

EXHIBIT A

LYON LIVING

4901 Birch Street
Newport Beach, CA 92660

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

January 29, 2025

NOTICE OF DATA INCIDENT

Dear <<Name 1>> <<Name 2>>:

Lyon Management Group, Inc. ("Lyon") is writing to make you aware of an event that may affect some of your information. This notice provides information about this event, our response, and resources available to you to help protect your information, should you feel it is appropriate.

What Happened? Lyon became aware of suspicious activity on our IT network. We took steps to secure our systems and began an investigation to determine the full nature and scope of the event. Our investigation determined that an unknown actor gained access to certain Lyon systems between March 14, 2024, and March 15, 2024, and potentially copied certain files from those systems during that period. We then undertook a thorough review of those files to determine what information was present and to whom it related. This review was completed on December 13, 2024. You are receiving this letter because we found your information in the relevant files.

What Information Was Involved? We determined that the following information related to you was in the relevant files: name and [insert data element]. We have no indication that there has been any actual or attempted fraud or identity theft as a result of the event.

What We Are Doing. Upon becoming aware of this event, we promptly began an investigation to determine the nature and scope of the event, took steps to secure our network, and notified federal law enforcement. As an added precaution, we are offering you access to 12 months of complimentary credit monitoring and identity restoration services through TransUnion. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. At this time, we are not aware of anyone experiencing fraud as a result of the event. In addition to enrolling in the complimentary monitoring services, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the attached *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information.

For More Information. If you have additional questions, please contact inquiries@lyon1.com.

Sincerely,

Lyon Management Group, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.