



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Brittany R. Bickel
Office: (267) 930-1129
Fax: (267) 930-4771
Email: BBickel@mullen.law

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

September 6, 2023

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 Real Estate (“Lyon”) located at 3640 American River Drive, Suite 100, Sacramento, California 95864, and write to notify your office of an event that may affect the security of certain personal information relating to one (1) Maryland resident. This notice may be supplemented if significant new facts are learned subsequent to its submission. 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 around May 4, 2023, Lyon identified suspicious activity related to its servers and systems within its main office building in Sacramento, California. Lyon immediately launched an investigation into the nature and scope of the event with the assistance of third-party subject matter specialists. Through the investigation, Lyon learned that an unknown individual accessed its systems via a software vulnerability in a vendor application program used by Lyon. The unauthorized access occurred at various times between April 18, 2023 and May 4, 2023, and the unauthorized actor obtained certain information stored in Lyon’s systems.

In an abundance of caution, Lyon worked with specialists to undertake a comprehensive review of information stored in the impacted files to determine what information was affected and to whom the information related. Lyon then conducted a manual review of its records to confirm the identities of individuals affected by this event and their contact information to provide notifications. This review was recently completed.

The information that could have been subject to unauthorized access related to the Maryland resident includes name, driver's license number, EIN/tax ID number, Social Security number, and financial information.

Notice to Maryland Resident

On or about September 6, 2023, Lyon began providing written notice of this event to potentially affected individuals, including one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Lyon moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals. Further, Lyon promptly reported the event to federal law enforcement. Lyon is also working to implement additional safeguards and training to its employees. Lyon is providing access to credit monitoring services for two (2) years, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Lyon is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Lyon is 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 providing written notice of this event to appropriate state regulators and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1129.

Very truly yours,

Brittany R. Bickel of
MULLEN COUGHLIN LLC

BRB/ogf
Enclosure

EXHIBIT A



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF <<SECURITY INCIDENT/DATA BREACH>>

Dear <<Name 1>>:

Lyon Real Estate (“Lyon”) is providing notice of an event that may affect some of your information. Although we have no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 4, 2023, Lyon identified suspicious activity related to its servers and systems within its main office building in Sacramento, California. We immediately launched an investigation into the nature and scope of the event with the assistance of third-party subject matter specialists. Through our investigation, we learned that an unknown individual accessed Lyon’s systems via a software vulnerability in a vendor application program used by Lyon. The unauthorized access occurred at various times between April 18, 2023 and May 4, 2023, and the unknown individual obtained certain information stored in Lyon’s systems.

In an abundance of caution, we worked with specialists to undertake a comprehensive review of information stored in the impacted files to determine what information was affected and to whom the information related. We then conducted a manual review of our records to confirm the identities of individuals affected by this event and their contact information to provide notifications. This review was recently completed.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the involved files at the time of the event: name and <<Data Elements>>.

What We Are Doing. We take this event and the security of information in our care seriously. Upon discovering this event, we promptly took steps to investigate and respond, assess the security of our systems, and notify potentially affected individuals. In response to this event, we are reviewing and enhancing our information security policies and procedures, which includes procedures with respect to the integration and use of third-party software products.

While we are unaware of any fraudulent misuse of your information as a result of this event, as an additional precaution, Lyon is offering you access to <<12/24>> months of complimentary credit monitoring and identity restoration services through Equifax. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits under your health insurance, and monitoring your free credit reports for suspicious activity and to detect errors.

Additional resources can be found below in the *Steps You Can Take to Help Protect Your Personal Information*. You may also enroll in the complimentary credit monitoring services being offered.

For More Information.

If you have additional questions, you may contact our dedicated assistance line toll-free at 844-675-4370. This toll-free line is available Monday through Friday 6:00 a.m. to 6:00 p.m. PST (excluding major U.S. holidays). You may also write to Lyon at Lyon Real Estate, 3640 American River Drive, Suite 100, Sacramento, CA 95864, Attn: Diana Murphy.

Sincerely,

Lyon Real Estate

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services



Enter your Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<ENROLLMENT DEADLINE>>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click "Submit" and follow these 4 steps:

1. Register:

Complete the form with your contact information and click "Continue".

If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. ²Credit monitoring from Experian and TransUnion will take several days to begin. ³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co ⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 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 <<RI #>> Rhode Island residents that may be impacted by this event.