

EXHIBIT 1

By providing this notice, Highlands Ranch Community Association (“HRCA”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 21, 2021, HRCA experienced a service disruption that was determined to be caused by a sophisticated cyber-attack. HRCA immediately launched an investigation to determine the nature and scope of this incident, working with outside cybersecurity specialists to securely restore its systems. The investigation determined on May 11, 2021 that a limited number of files and folders within the HRCA environment that were accessed by the unknown actor. HRCA then performed a programmatic and manual review of the contents of the files and folders to determine whether sensitive information was present within them. This process completed on September 24, 2021. HRCA then worked diligently to locate address information for the affected individuals and just recently completed that effort.

The information that could have been subject to unauthorized access includes name, address, and financial account information.

Notice to Maine Residents

On or about October 21, 2021, HRCA provided written notice of this incident to affected individuals, which includes two (2) Maine 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

Upon discovering the event, HRCA moved quickly to investigate and respond to the incident, assess the security of HRCA systems, and notify potentially affected individuals. HRCA is also working to implement additional safeguards and training to its employees. HRCA is providing access to credit monitoring services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HRCA is providing impacted 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. HRCA 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.

EXHIBIT A

<Return Name>
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

Re: Notice of Data Breach

Dear [insert name]:

Highlands Ranch Community Association, Inc. (“HRCA”) writes to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On or about March 21, 2021, HRCA experienced a service disruption that was later determined to be caused by a sophisticated cyber-attack. We immediately launched an investigation to determine the nature and scope of this incident, working with outside cybersecurity specialists. The investigation determined on May 11, 2021, that a limited number of files and folders within the HRCA environment may have been accessed during this event. We then performed a programmatic and manual review of the contents of the files and folders to determine whether sensitive information was present within them. This process completed on September 24, 2021. HRCA then worked diligently to locate address information for the affected individuals and just recently completed that effort.

What Information Was Involved? The investigation determined that the following types of your personal information were present in the files and folders accessed by the unknown actor at the time of the incident: name and [Variable Text 1].

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained personal information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. We also notified and are cooperating with Federal law enforcement. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

We are also offering you access to complimentary credit monitoring and identity protection services for 12 months through Kroll. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you. While HRCA will cover the cost of these services, we are not able to enroll on your behalf and you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at [number and hours of operation].

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Gerald Flannery
CEO/GM
Highlands Ranch Community Association, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration

[Credit/Identity Monitoring Instructions]

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

Should you wish to place a fraud alert or credit freeze, 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
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You

can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Highlands Ranch Community Association, Inc. is located at 9568 South University Boulevard, Highlands Ranch, CO 80126-2912.

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, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit 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 violator. You 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 you to review your 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>