Dinsmore

Legal Counsel.

DINSMORE & SHOHL LLP
255 E. Fifth Street ^ Suite 1900
Cincinnati, OH 45202
www.dinsmore.com

Kurt R. Hunt
(513) 977-8101 (direct) ^ (513) 977-8141 (fax)
kurt.hunt@dinsmore.com

April 15, 2021

VIA CERTIFIED MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notice of Data Breach

To Whom It May Concern:

Dinsmore & Shohl LLP represents Resort Lifestyle Communities ("RLC"). RLC operates all-inclusive resort-style communities to provide independent living for adults age 55 and over. I am writing to inform your office of a recent security incident experienced by RLC that may have exposed personal information.

On or about February 6, 2021, RLC discovered it was the victim of a ransomware attack that encrypted portions of its systems. Upon discovery of the security incident, RLC engaged a digital forensic firm and legal counsel, and initiated an investigation to understand the scope and nature of the security incident. RLC maintains robust data backups and was able to recover nearly all data contained in the affected systems. Accordingly, RLC decided not to pay the threat actor to decrypt its systems.

In the course of its investigation, RLC determined that in addition to encrypting portions of its systems, the threat actor may have exfiltrated some of its information. RLC confirmed the data exfiltration on February 12, 2021 when portions of information maintained by RLC were published on the threat actor's public website. RLC and its retained digital forensic firm analyzed both the information published by the threat actor and the encrypted portions of its systems to determine the scope of the threat actor's access to personal information. As a result of this review, it was determined that some personal information may have been accessed by the threat actor. RLC did not complete its forensic investigation and determine the full scope of access to personal information until on or about February 25, 2021.

The forensic investigation was able to identify with substantial—but not complete—certainty the threat actor's entry vector(s) to RLC's systems. Thereafter,

RLC evaluated its several systems and subfolders to attempt to identify the populations of individuals affected and the specific types of personal information that may have been exposed. The forensic investigation and subsequent evaluation of systems and subfolders provided limited indications of what types of information the threat actor may have accessed. Ultimately, RLC, acting under a "worst case scenario" ethos, determined that the types of personal information that may have been accessed included first name, last name, social security number, bank account number, and bank routing number. In total, 14,700 individuals associated with RLC were affected, including 8 New Hampshire residents.

Per applicable state data breach notification laws, RLC notified the three major consumer reporting agencies of the security incident on April 15, 2021. In addition, RLC will provide all affected individuals notice of the security incident via U.S. mail on April 15, 2021. There is a small subset of potentially affected individuals we continue to investigate to determine whether they were impacted by the security incident. If RLC's investigation concludes that these individuals were impacted, RLC will notify them of the security incident immediately.

We are offering affected individuals with potentially exposed social security numbers identity monitoring services for one year, at no cost to the affected individual, through Kroll. Residents of Connecticut and Massachusetts will be offered identity monitoring services for two years pursuant to applicable state data breach notification requirements. These services include credit monitoring, fraud consultation, and identity theft restoration. We have also established a call center through Kroll to help route questions about the security incident to RLC and respond to any questions affected individuals may have about identity monitoring services being offered. A copy of the individual data breach notification letter, along with instructions for how affected individuals can register for identity monitoring services, is enclosed with this letter.

Since discovering the security incident, RLC initiated remedial measures to further safeguard customer personal information. These measures included, among other measures, retaining forensic experts to determine the scope of the security incident and eliminate any unauthorized access, installing threat monitoring technologies, and exploring the deployment of a SIEM with company-wide input for network access visibility. We are also reviewing our existing data practices, policies, and procedures to protect our information and systems further, including by broadening our use of multi-factor authentication measures, implementing access limitations to certain data and systems, and migrating certain information to a secure third-party cloud provider. RLC will be working with privacy legal counsel to review its existing policies and procedures to identify additional areas of improvement.

If you have any additional questions or require more information, you can reach me by email at kurt.hunt@dinsmore.com or by phone at (513) 977-8101.

Sincerely,

/s/ Kurt R. Hunt

Kurt R. Hunt

Enclosure

RLC
RESORT LIFESTYLE COMMUNITIES

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

**Notice of Data Breach**

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

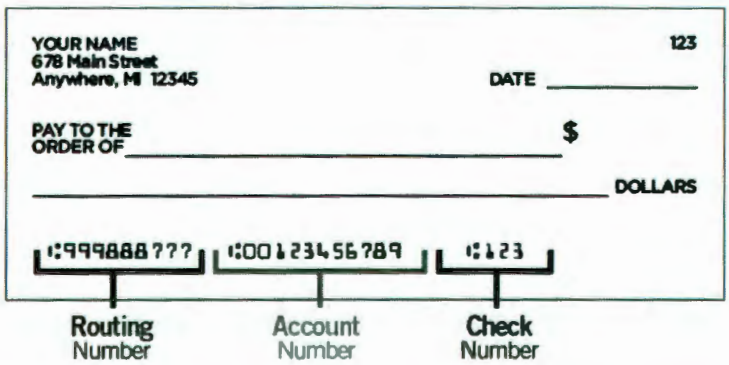
Resort Lifestyle Communities ("RLC") is writing to inform you of a recent security incident that may have exposed your personal information and to provide you information on steps you can take to help protect your personal information.

***What Happened?***

On or about February 6, 2021, RLC discovered it was the victim of a cyber-attack. Upon discovery of the security incident, RLC engaged a digital forensics firm to conduct an investigation into the scope of the security incident.

***What Information Was Involved?***

In the course of the investigation, RLC determined that some of your information may have been accessed during the security incident. The type of information that may have been accessed includes your first name, last name, Social Security number, bank account number, and bank routing number. Bank account and routing numbers are pieces of information used to facilitate payments. This information is generally found at the bottom of standard bank check as seen below:




**RLC does not collect or maintain bank security codes, access codes, pin numbers, and passwords. RLC is currently unaware of any misuse of your information as a result of the security incident.**

***What We Are Doing***

Following discovery of the security incident, RLC immediately initiated remedial security measures to further safeguard your personal information. These measures included, among others, retaining forensic experts to determine the scope of the security incident and eliminate any unauthorized access. RLC will continue to take measures to ensure the security of your information and evaluate other security enhancements it can implement to protect against similar incidents in the future.

***What You Can Do***

Please review the attached supplement (*Steps You Can Take to Help Protect Your Information*) for additional steps you can take to further protect your personal information. If you are concerned about the security of your bank account, please contact your financial institution or company with which your account is maintained. In addition, RLC has secured

the services of Kroll to provide identity monitoring services to you at no cost for 1 year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience assisting with data breach response. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

You have until **July 16, 2021** to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

Additional information describing your services is included in the attached supplement. RLC has also established a call center with Kroll to respond to any questions you may have about the identity monitoring services offered to you. Please call 1-855-935-6099, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time with any questions. Please have your membership number ready.

***For More Information***

If you have any questions about the security incident, please contact RLC by phone at (402) 420-2311, Monday through Friday from 9:00 a.m. to 5:00 p.m. Central Time.

Sincerely,

Resort Lifestyle Communities
7101 S. 82nd Street
Lincoln, NE 68516
(402) 420-2311
www.rlcommunities.com

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**Take Advantage of Your Credit Monitoring Services.** You have been provided with access to the following services from Kroll:

**Single Bureau Credit Monitoring:** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

**Fraud Consultation:** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration:** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

*Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.*

You can take the following additional steps to protect your information:

**Contact Information for the three Nationwide Credit Reporting Agencies.**

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| PO Box 740241 | PO Box 2104 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-685-1111 | 1-888-397-3742 | 1-800-888-4213 |

**Free Credit Report.** It is recommended that you remain vigilant over the next twelve to twenty-four months by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft.

It is recommended that you periodically obtain and review a copy of your credit report from each of the three nationwide credit reporting agencies, and have any information relating to fraudulent transactions deleted. You may obtain a copy of your credit report, free of charge, once every twelve months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Your Rights Under the Fair Credit Reporting Act.** You have several rights related to the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. To learn more about your rights under the Fair Credit Reporting Act, please visit www.consumerfinance.gov/learnmore/ or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

**Fraud Alerts.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security Freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone

line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

**Federal Trade Commission and Additional Identity Theft Resources.** 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 the Federal Trade Commission ("FTC"). You may contact the FTC by phone at 1-877-IDTHEFT (438-4338) or by mail at Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You may also visit www.identitytheft.gov.

In addition, the FTC provides additional resources with steps you can take to protect against identity theft. For more information, please visit www.ftc.gov/bcp/edu/microsites/idtheft/. A copy of *Taking Charge: What to Do if Your Identity is Stolen*, a comprehensive guide from the FTC to help you guard against and deal with identity theft is available on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

**IRS Identity Protection PIN.** The Internal Revenue Service ("IRS") offers the option to create an Identity Protection PIN ("IP PIN") to prevent someone else from filing a tax return using your Social Security number. The IP PIN is a six-digit number known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. For more information on how you can opt-in to using an IP PIN, please visit www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

**State Attorneys General Offices.** 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 the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106; www.ct.gov/ag; 1-860-808-5318.

**For D.C. residents:** You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001; https://oag.dc.gov/consumer-protection; 1-202-442-9828.

**For Iowa residents**: You may contact the Office of Attorney General of Iowa, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319; https://www.iowaattorneygeneral.gov/for-consumers; 1-515-281-5926.

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; https://www.marylandattorneygeneral.gov/; 1-888-743-0023.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108; www.mass.gov/ago/contact-us.html; 1-617-727-8400.

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

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; www.ncdoj.gov; 1-877-566-7226.

**For Oregon residents**: You may contact the Oregon Office of the Attorney General, 1162 Court St. NE, Salem, OR 97301-4096; www.doj.state.or.us/; 1-877-877-9392.

**For Rhode Island residents**: You may contact the Rhode Island Office of the Attorney General, 150 S. Main St., Providence, RI 02903; http://www.riag.ri.gov/; 1-401-274-4400.

**Reporting of Identity Theft and Obtaining a Police Report.** Please review your account statements for any suspicious activity. If you detect any suspicious activity on an account or suspect identity theft, you should immediately report it to the financial institution or company with which the account is maintained. You have the right to obtain any police report filed concerning this incident. If you are the victim of identity theft, you also have the right to file and obtain a copy of a police report.

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

**For Rhode Island residents:** You have a right to obtain a police report if you are a victim of identity theft.