Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

September 19, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent REDICO Management, Inc. ("REDICO"), One Towne Square, Suite 1600 Southfield, MI 48076 and its affiliate, American House and write to notify your office of an incident that may affect the security of personal information relating to approximately one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, REDICO does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On September 11, 2018 REDICO discovered that W-2 information from 2017 of current and former employees were fraudulently obtained through a cyber-security incident on September 10, 2018. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was impacted by this event. Since discovering the event, REDICO has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Resident

On or around September 19, 2018 REDICO began providing written notice of this incident to potentially affected individuals, which includes approximately one (1) New Hampshire resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

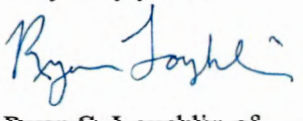
Other Steps Taken and To Be Taken

Upon discovering the spoofed email, REDICO immediately launched an investigation to determine the nature and scope of this incident, as well as determine the identities of the individuals potentially affected. REDICO is providing written notice to those individuals who may be affected by this incident. This notice will include an offer of complimentary access to one (1) year of credit and identity monitoring services, including identity restoration services through ID Experts, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, REDICO is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. REDICO will also be providing notice of this event to other entities as may be required under the applicable state laws.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:emp
Enclosure

EXHIBIT A

American House
SENIOR LIVING COMMUNITIES

To Enroll, Please Call:
(844) 322-8152
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: [XXXXXXXX]

C/O ID Experts
PO Box 10444
Dublin, Ohio 43017-4044

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

September 19, 2018

Dear <<FirstName>> <<LastName>>:

I am writing to inform you that data from your 2017 W2 was improperly accessed through a recent cyber-security incident. Unfortunately, we are not alone in this regard. Some of the largest and most highly regarded companies in the world, like Experian, Equifax, Target, Sony, Panera Bread, and Facebook, have all experienced cyber-attacks. We take this incident very seriously and as a precaution, we are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On September 11, 2018, we discovered that W-2 information from 2017 of current and former employees were fraudulently obtained through a cyber-security incident on September 10, 2018. We took immediate steps to mitigate any potential impact and began an investigation into this incident.

What Information Was Involved? A copy of your 2017 IRS Tax Form W-2, was improperly obtained. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was obtained.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. American House has and is taking steps to prevent this type of cyber-attack from happening in the future.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of triple bureau credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. The cost of this service will be paid for by American House.

What You Can Do. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (844) 322-8152 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday 8:00 a.m. – 8:00 p.m. ET. Please note the deadline to enroll is December 19, 2018.

MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. You can also review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud".

In addition, if you have not already done so, we encourage you to file your 2017 tax return as soon as possible. If you become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039 Identity Theft Affidavit along with a paper copy of your return and mail according to the instructions on that form. A copy of this form can be found at: https://www.irs.gov/pub/irs-pdf/f14039.pdf, or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

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 dedicated assistance line at (844) 322-8152 (toll free), Monday through Friday, 8:00 a.m. to 8:00 p.m. ET. This will be your only source for information concerning the cyber-attack.

We take the privacy and security of the personal information in our care seriously, and sincerely regret any inconvenience or concern this incident may cause you. We are sincerely sorry this happened.

Sincerely,

Kari Lawry
Chief Human Resources Officer
American House

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

File Your Tax Return. If you have note already done so, we encourage you to file your 2017 tax return as soon as possible. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies.

Credit Reports. 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. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee up until September 21, 2018 to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. After September 21, 2018 you should not be charged a fee to place or lift a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.