HOMEBRIDGE

1035 Market Street, L-1
San Francisco, CA 94103
(T) 415.255.2079
(F) 415.255.0679
www.homebridgeca.org

April [date], 2015

«FirstName» «LastName»
«Address_1»
«Address_2»
«City», «State» «Zip»

Dear «FirstName»,

Homebridge, formerly the In-Home Supportive Services ("IHSS") Consortium, is writing to notify you of a data security incident that may have resulted in the compromise of the personal information of certain current and former Homebridge employees. Homebridge has discovered that cyber criminals deployed malicious software, or "malware," on a limited number of Homebridge computers, which may have allowed the criminals to obtain unauthorized access to certain human resource ("HR") records. Homebridge believes that the approximate date of the unauthorized access to the HR records in question may have been between January and March 2015. The personal information that was potentially accessed includes first and last name, address, and social security number. Homebridge has received reports that criminals may have used the stolen information to file fraudulent tax return forms with the Internal Revenue Service ("IRS") on behalf of Homebridge employees.

Homebridge takes its responsibility to protect your privacy seriously. Homebridge has retained a leading data forensics and cybersecurity firm to assist in its investigation of this incident and has taken steps to eradicate the malware and further enhanced the security of its systems. Homebridge is also fully cooperating with U.S. law enforcement to help bring the criminals involved to justice.

Homebridge regrets that this incident may affect you. Therefore, Homebridge is alerting you so that you can take steps to protect yourself from possible identity theft. Homebridge encourages you to:

1. Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion) to place a fraud alert on your credit file, requesting that creditors contact you before they open any new accounts or change your existing accounts;

2. Monitor your credit reports;

3. Review your credit card, debit card, bank statements and your federal and state tax filings for any unauthorized transactions or filings;

4. Notify your financial institution if you discover any unauthorized purchases or cash advances and report any fraudulent activity or any suspected incidence of identity theft to law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"); and

5. Close any accounts that you believe have been tampered with or opened fraudulently.

As part of Homebridge's commitment to its employees, Homebridge is also offering one year of identity protection and credit monitoring services from ID Guard at no cost to you. To enroll in ID Guard, call [toll free number] or go to [website] and follow the instructions. The promotion code required to use this free service is [Homebridge], and your personalized Member ID is your last name plus the last four digits of your social security number. Please note that you will have until 30 days after the date of delivery of this letter to enroll in this service.

Homebridge recommends that you remain vigilant even if you do not find any suspicious activity at this time and check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus.

If you find suspicious activity on your credit reports or have reason to believe that your information is being misused, call your local police department and file a police report. You should save a copy of the report; some creditors may want the information it contains to absolve you of fraudulent debts. You can also file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.

If you have questions, please contact HR at (415) 659-5331. For further details on steps you can take to protect your personal information, please review the attached guide.

Sincerely,

Mark Burns
Deputy Director

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Homebridge is providing this reference guide to assist individuals who believe their personal information may have been compromised. Homebridge encourages you to remain vigilant, review payment card account statements, monitor credit reports, and consider these additional steps.

Review Your Account Statements

As a precautionary measure, Homebridge recommends that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Credit Reports

To order a free copy of your credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the FTC website at http://www.ftc.gov/bcp/edu/resources/forms/requestformfinal.pdf and mail it to:

Annual Credit Report Request Service,
P.O. Box 105281,
Atlanta, GA 30348-5281

The three national credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be internally reviewed and, if

found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

Consulting the FTC

If you detect any incident of fraud, promptly report the incident to your local law enforcement authority, your state Attorney General and the FTC. If you believe your account has been compromised, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. When you dispute new unauthorized accounts, use the FTC's ID Theft Affidavit, which is available at http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the crime.

You can contact the FTC to learn more about how to protect yourself:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Police Report

If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as creditors may request such documentation to waive your potential liabilities in connection with fraudulent activity.

Fraud Alerts

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert notifies you of an attempt by an unauthorized person to open a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. An initial fraud alert is free and will stay on your credit file for at least 90 days. You can place a free fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. You can also place a fraud alert on your credit report online at the websites listed below.

Equifax	Experian	TransUnion
Phone: 800-525-6285 P.O. Box 105069 Atlanta, GA 30348-5069 http://www.equifax.com/answers/set-fraud-alerts/en_cp	Phone: 888-397-3742 P.O. Box 9532 Allen, TX 75013 https://www.experian.com/fraud/center_rd.html	Phone: 800-680-7289 P.O. Box 6790 Fullerton, CA 92634-6790 https://fraud.transunion.com

Security Freeze

Some state laws allow you to place a security freeze on your credit reports. A security freeze would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, 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. The specific costs and procedures for placing a security freeze vary by state. You can find additional information at the websites of any of the three credit reporting agencies listed below.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, the agency will not charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you a fee, which generally ranges from $5.00 to $20.00 per action.

Requirements vary by state, but generally you may place a security freeze on your credit report by sending a written request to each of the three credit reporting agencies noted below, which may require the following information to verify your identity:

(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 five years;
(5) proof of current address; and
(6) a legible copy of a government issued identification card.

You also may provide a copy of any relevant police report, investigative report, or complaint to a law enforcement agency concerning the incident.

Equifax	Experian	TransUnion
Phone: 800-525-6285 P.O. Box 105788 Atlanta, Georgia 30348	Phone: 888-397-3742 Experian Security Freeze P.O. Box 9554	Phone: 800-680-7289 P.O. Box 6790 Fullerton, CA 92634-6790

http://www.equifax.com/answers/help/security-freeze/en_cp	Allen, TX 75013 www.experian.com/freeze	https://freeze.transunion.com

Tax-Related Identity Theft

Step #1 — Open an IRS online account and view your records on-line at http://www.irs.gov/Individuals/Get-Transcript. Choose to view transcripts online and register for an account. The IRS will send a confirmation code to the email account you register. With that code, you can then answer the security questions and gain access to your past several years of tax records online. If there is an entry for this tax year and you have not filed a tax return form, this could be a fraudulent filing. Click on the Record of Account and print out a copy of the forms.

Step #2 — If there are signs of fraudulent activity, go to this link: http://www.irs.gov/Individuals/How-Do-You-Report-Suspected-Tax-Fraud-Activity%3F. Specifically, on this page you are looking for this information:

…suspect someone **stole your identity and used your SSN** for employment purposes or could use your SSN to file a tax return	Use Form 14039* *Spanish version: Form 14039SP	Complete the form online, print it and mail or fax to the appropriate office using the options listed on page 2 of the form. Include photocopies of at least one of the documents listed on the form to verify your identity. For additional information, refer to the Taxpayer Guide to Identity Theft

Form 14039 (or 14039SP for Spanish) is the form you should use to inform the IRS that you have been a victim of identity theft. The form includes detailed instructions on how it should be filled out — most commonly you will attach the form to the top of your paper tax returns and mail them in to the IRS. If you have other correspondence with fax or mail information, you can send the form to that address/fax instead.

Also, if you are a victim of identity theft, the following link provides information on other steps to take to begin to correct the potential damage and to help ensure that no further damage can be done by the perpetrators of these crimes - http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. Further information regarding tax-related identity protection is available at http://www.irs.gov/Individuals/Identity-Protection. Tax-related identity theft information is also available on the FTC's website at http://www.consumer.ftc.gov/articles/0008-tax-related-identity-theft.

Resources from the State of California

California's Attorney General's Office provides data breach help and tips for consumers on their website at https://oag.ca.gov/privacy/other-privacy/breach-help-tips-for-consumers.

You can also contact California's Attorney General's Office at:

Attorney General's Office
California Department of Justice
Attn: Office of Privacy Protection
P.O. Box 944255
Sacramento, CA 94244-2550
Telephone: (916) 322-3360
Toll-free in California: (800) 952-522

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

A copy of Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC to help you guard against and deal with identity theft, is available at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.