August 30, 2023

VIA MAIL

Maryland Office of the Attorney General
Attn: Data Breach Notification
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Re: Notification Pursuant to Md. Code Com. Law § 14-3501 *et seq.*

Dear Office of the Attorney General:

Pursuant to Md. Code Com. Law § 14-3501 *et seq.*, I am writing on behalf of HomeServe USA Corp. ("HomeServe"), located at 601 Merritt 7, Norwalk, CT 06851, to notify you of a breach of security involving the personal information of one (1) Maryland resident.

HomeServe recently identified some suspicious activity involving its employee data stored on HomeServe's third-party, cloud-based human resources ("HR") and payroll platform and initiated an investigation to determine the scope of the issue. Through its investigation, HomeServe determined that an unknown and unauthorized third party utilized sophisticated social-engineering tactics to access certain users' accounts on HomeServe's HR and payroll platform between July 25, 2023 and August 1, 2023. This unidentified third party attempted, unsuccessfully, to redirect a portion of the paychecks for a limited number of our employees into fraudulent accounts and, in doing so, could have viewed certain sensitive employee information stored on our HR and payroll platform. The information that was accessed by this third party is limited to name and bank account and routing number.

As a precautionary measure, HomeServe has provided the one affected Maryland resident with credit monitoring and identity protection services through LifeLock at no charge for a period of twenty-four (24) months. HomeServe has also included direct contact information for the internal points-of-contact at HomeServe who have knowledge of this incident and will be able to answer any questions the individual may have about the incident or the services available. Enclosed is a template copy of the written notice that will be sent via mail to that individual subsequent to this notice on August 31, 2023, pursuant to Md. Code Com. Law § 14-3504(b)(2).

HomeServe maintained a written information security program ("WISP") at the time of the incident and is currently evaluating and updating, as appropriate, its WISP. In response to this incident, HomeServe disabled the relevant portions of its HR and payroll platform to help prevent further unauthorized access and ensured that all user account passwords to the system were changed. HomeServe has also implemented additional layers of security around user access to the platform, such as multi-factor authentication, and enhanced verification procedures for requests to reset user account passwords.

HomeServe

If you have any further questions or require further information, please do not hesitate to contact me.

Very truly yours,

Elizabeth A. Sauvigne

Elizabeth A. Sauvigne
Asst. General Counsel, Legal & Compliance
Data Privacy Officer
T: 203-970-7225
elizabeth.sauvigne@homeserveusa.com

Enclosure:
Sample Copy of Notice Letter

HomeServe

HomeServe USA Corp.
601 Merritt 7
Norwalk, CT 06851

[NAME]
[ADDRESS]
[CITY] [STATE] [ZIP]

August 30, 2023

Dear [NAME]:

At HomeServe USA Corp. ("HomeServe"), we value and respect the privacy of your personal information. We are writing to follow up with you regarding a recent security incident that involved some of your personal information and to share some steps that you can take to help protect your information.

WHAT HAPPENED?

As you know, we recently identified some suspicious activity involving our employees' data stored on HomeServe's third-party, cloud-based human resources ("HR") and payroll platform and initiated an investigation to determine the scope of the issue. Through our investigation, we determined that an unknown and unauthorized third party utilized sophisticated social-engineering tactics to access your account on HomeServe's HR and payroll platform between July 25, 2023 and August 1, 2023. This unidentified third party attempted, unsuccessfully, to redirect the paychecks for a limited number of our employees into fraudulent accounts and, in doing so, could have viewed certain sensitive employee information stored on our HR and payroll platform.

WHAT INFORMATION WAS INVOLVED?

The information involved in this incident is limited to your name and bank account and routing numbers.

WHAT WE ARE DOING.

Upon learning of this issue, we disabled the relevant portions of our HR and payroll platform to help prevent further unauthorized access and ensured that all user account passwords to the platform were changed. In response to this incident, we have also implemented additional layers of security around user access to the platform, such as multi-factor authentication, and enhanced verification procedures for requests to reset user account passwords.

WHAT YOU CAN DO.

To help relieve any concerns and restore your confidence in HomeServe following this incident, we have arranged for you to enroll in two (2) years of credit monitoring and identity theft protection, free of charge, through LifeLock's "Ultimate Plus" plan. You may sign up for this service by following the instructions attached to this notice.

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your 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. We also encourage you to review the supplemental information attached to this notice, as it describes additional measures you can take to protect your information, including recommendations by the U.S. Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit report.

FOR MORE INFORMATION.

For further information and assistance, please reach out to a member of our Data Privacy Team, Elizabeth Sauvigne or MaryKate Mrazik Bassoli, via the contact information below.

Elizabeth A. Sauvigne
Asst. General Counsel, Legal & Compliance
Data Privacy Officer
T: 203-970-7225
elizabeth.sauvigne@homeserveusa.com

MaryKate Mrazik Bassoli
Senior Marketing & Privacy Counsel
T: 203-957-4634
MaryKate.MrazikBassoli@HomeServeUSA.com

Sincerely,

Cherie Sheridan
Chief People Officer
HomeServe USA Corp.

HomeServe

Steps You Can Take to Further Protect Your Information

1. Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the major credit reporting agencies once every twelve (12) months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action.

You can also elect to purchase a copy of your credit report by contacting one of the national credit reporting agencies. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	**Experian**	**TransUnion**	**Innovis**
(866) 349-5191	(888) 397-3742	(800) 888-4213	(800) 540-2505
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000	P.O. Box 1689
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022	Pittsburgh, PA 15230
www.equifax.com	www.experian.com	www.transunion.com	www.innovis.com

2. Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing an initial or extended fraud alert on your credit report, at no charge, by contacting any of the credit reporting agencies. An initial fraud alert will stay on your credit file for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for seven (7) years, on your credit report. To place a fraud alert on your credit report, contact any of the credit reporting agencies identified below:

Equifax	**Experian**	**TransUnion**	**Innovis**
(800) 525-6285	(888) 397-3742	(800) 680-7289	(800) 540-2505
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000	P.O. Box 26
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Pittsburgh, PA 15230
www.equifax.com/ personal/credit-report-services/ credit-fraud-alerts	www.experian.com/ fraud/center.html	www.transunion.com/ fraud-alerts	www.innovis.com/personal/ fraudActiveDutyAlerts

3. Consider Placing a Security Freeze on Your Credit Report

You have the right to place, lift, or remove a security freeze on your credit report, free of charge. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

HomeServe

You must place your request for a freeze with each of the following consumer reporting agencies. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail to the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax (800) 349-9960 P.O. Box 105788 Atlanta, GA 30348 www.equifax.com/personal/credit-report-services/	**Experian** (888) 397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze/center.html	**TransUnion** (888) 909-8872 P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze	**Innovis** (800) 540-2505 P.O. Box 26 Pittsburgh, PA 15230 www.innovis.com/personal/securityFreeze

To place a security freeze, you may be required to provide the consumer reporting agency with some or all of the following information, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): full name (with middle initials and any suffixes); Social Security number; date of birth; current and previous addresses for the past five years; a copy of your state-issued identification card, Social Security Card, pay stub, or W2; any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles; and a recent utility bill, bank statement, or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or up to three (3) business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social

Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

4. Federal Trade Commission and State Attorneys General

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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **Maryland residents**, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft by visiting https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.
- **New York residents**, you may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General by calling 1-800-771-7755 or visiting https://ag.ny.gov; the New York State Police by calling 1-518-457-6721 or visiting https://troopers.ny.gov/; and/or the New York Department of State by calling 1-800-697-1220 or visiting https://www.dos.ny.gov.
- **Oregon residents**, you are advised to report any suspected incidents of identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

5. Credit Report Monitoring/Identity Theft Protection Services

HomeServe will be providing you with credit monitoring and identity theft protection services for two (2) years through LifeLock's "Ultimate Plus Plan", at no cost to you. **To take advantage of this offer, you must enroll by October 29, 2023.** Once you have enrolled, please submit your receipt to payroll@homeserveusa.com for reimbursement, if you have not done so already. In addition, please do not hesitate to reach out if you require assistance from HomeServe to enroll in the coverage. For information on LifeLock "Ultimate Plus" Membership and to sign up, refer to LifeLock's website at https://lifelock.norton.com/products/lifelock-ultimate-plus. Your use of LifeLock's services is subject to LifeLock's terms and conditions.