

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

From: Vaughn, Lael (CLE-NA) <Lael.Vaughn@bshg.com>
Sent: Wednesday, January 20, 2021 4:15 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: BSH Customer Notice

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

Name and contact information of person reporting the breach.
Lael Vaughn, Associate General Counsel
Lael.vaughn@bshg.com

BSH Home Appliances Corporation, 1901 Main Street, Suite 600, Irvine, CA 92614

o Name and address of business that experienced the breach, and the type of business.

BSH Home Appliances Corporation, 1901 Main Street, Suite 600, Irvine, CA 92614
Home Appliances Manufacturer

o A general description of the breach, including the date(s) of the breach, when and how the breach was discovered, and any remedial steps taken in response to the breach.

BSH operates a call center for its brands that customers can use to request parts, make warranty claims or ask for technical assistance. In early December 2020, BSH determined based on its investigation of several customer complaints regarding unauthorized credit card transactions that unbeknownst to BSH, a temporary employee had been improperly requesting credit card information from callers and using that information to make unauthorized purchases. It further determined that unbeknownst to BSH, this particular temporary employee had been requesting credit card information from callers and using that information to make unauthorized purchases. To date, BSH has only confirmed that the incident affected four customers. BSH promptly terminated the employee as such collection and use was not authorized and contrary to BSH policies.

o The number of New Hampshire residents affected by the breach.

4

o A detailed list of the categories of personal information subject of the breach.

The personal information potentially misused includes: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country and Credit Card information (including card number, expiration date and CVV Code).

o The date(s) that notification was/ will be sent to the affected New Hampshire residents.

January 20, 2021

o A template copy of the notification sent to the affected New Hampshire residents.

Attached.

o Whether credit monitoring or identity theft protection services has been or will be offered to affected New Hampshire residents, as well as a description and length of such services.

Credit monitoring provided by Identity Guard for a period of one year will be provided to consumers. Details included in attached notification to residents.

Kind regards,
Lael A. Vaughn

BSH Home Appliances Corporation
Associate General Counsel

1901 Main Street, Suite 600
Irvine, CA 92614
Tel.: 949.862.3138
lael.vaughn@bshg.com
www.bsh-group.com/us/

January 20, 2021

«First_Name» «Last_Name»
«Address»
«City», «State» «Zip_Code»
«Email»

NOTICE OF DATA BREACH

On behalf of BSH Home Appliances Corporation (“BSH”) we are writing to inform you about a recent incident involving the potential misuse of some of your personal information that you may have provided while contacting our call center.

WHAT HAPPENED?

BSH operates a call center for its brands that customers can use to request parts, make warranty claims or ask for technical assistance. In early December 2020, BSH determined based on its investigation of several customer complaints regarding unauthorized credit card transactions that unbeknownst to BSH, a temporary employee had been improperly requesting credit card information from callers and using that information to make unauthorized purchases. It further determined that unbeknownst to BSH, this particular temporary employee had been requesting credit card information from callers and using that information to make unauthorized purchases. To date, BSH has only confirmed that the incident affected four customers. BSH promptly terminated the employee as such collection and use was not authorized and contrary to BSH policies.

WHAT INFORMATION WAS INVOLVED?

The personal information potentially misused includes: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country and Credit Card information (including card number, expiration date and CVV Code).

WHY ARE WE CONTACTING YOU?

Although BSH has only documented four customers whose information might have been misused to date, BSH is contacting all individuals whose call was handled by this temporary employee and it appears the consumer may have provided personal information during their call.

WHAT ARE WE DOING?

BSH promptly terminated the temporary employee suspected of collecting and misusing the credit card information. It also promptly notified the FBI and the local authorities about the incident. BSH also intends to implement further training and screening procedures to ensure that call center employees are not collecting any such information, unless required for a transaction.

As an added safeguard, we have arranged for you, at your option, to enroll, at no cost to you, in an online credit monitoring service -- Identity Guard. A description of this service is provided in

the attached material, which also contains instructions about how to enroll including your personal activation code. Please note that you must enroll to take advantage of this free service and we encourage you to do so. We strongly recommend you consider enrolling in this product, at our expense, and review the additional material enclosed with this letter.

WHAT YOU CAN DO?

1. **Sign Up for Credit Monitoring.** We encourage you to take advantage of the complimentary credit monitoring services we are providing. As noted above, a description of the credit monitoring services is provided in the attached material.
2. **Monitor Account Statements and Free Credit Reports.** You should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your credit card and debit card account statements and monitoring free credit reports (please see Section 4 below for more information).
3. **Contact the Federal Trade Commission, Law Enforcement, and Credit Bureaus.** You may contact the Federal Trade Commission (“FTC”), your state’s Attorney General’s office, or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s websites at www.IdentityTheft.gov and www.consumer.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide credit reporting agencies at:

Equifax
(800) 525-6285
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9701 Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com

4. **Obtain a Free Copy of Credit Reports.** You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete

that information from your credit report file. In addition, under the Fair Credit Reporting Act (“FCRA”), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.

5. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax: (800) 349-9960
Experian: (888) 397-3742
TransUnion: (888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.;
- Social Security number;
- Date of birth;
- Current address and all addresses for the past two years;
- Proof of current address, such as a current utility bill or telephone bill;
- Legible copy of a government-issued identification card, such as a state driver’s license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. You may contact us at the following email if you have any questions or concerns: data-response@bshg.com.

ADDITIONAL CONTACT INFORMATION

IF YOU ARE A COLORADO RESIDENT: You may also obtain information about preventing identity theft from the Office of the Attorney General. This office can be reached at: Office of the Attorney General, Consumer Protection Section, Colorado Department of Law, Ralph L. Carr Judicial Building, 1300 Broadway, 7th Floor, Denver, CO 80203, <https://www.stopfraudcolorado.gov/fraud-center/identity-theft.html>. For immediate assistance, you may call the Colorado Bureau of Investigation's 24 Hour Identity Theft & Fraud Hotline at 1-855-443-3489.

IF YOU ARE AN ILLINOIS RESIDENT: You may also obtain information about preventing identity theft from the Consumer Protection Division of the Illinois Attorney General's office. This office can be reached at: Illinois Attorney General, Consumer Fraud Bureau, 500 South Second Street, Springfield, IL 62701, 1-800-243-0618. You may also call the identity theft hotline at 1-877-844-5461, <https://illinoisattorneygeneral.gov/consumers/filecomplaint.html>.

IF YOU ARE AN IOWA RESIDENT: You may also obtain information about preventing identity theft and report suspected incidents of identity theft to local law enforcement and the Iowa Attorney General's Office. This office can be reached at: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 515-281-5926, consumer@ag.iowa.gov. Further information is available at <https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft>.

IF YOU ARE A MASSACHUSETTS RESIDENT: You may also obtain information about preventing identity theft from the Office of Consumer Affairs and Business Regulation. This office can be reached at: Office of Consumer Affairs and Business Regulation, 501 Boylston St., Suite 5100, Boston, MA 02116, (888) 283-3757, <https://www.mass.gov/orgs/office-of-consumer-affairs-and-business-regulation>. You also have the right to obtain a police report if you are the subject of identity theft.

IF YOU ARE A MARYLAND RESIDENT: You may also obtain information about avoiding identity theft and recommended next steps if you are the subject of identity theft from the Maryland Attorney General's Office. This office can be reached at: Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

IF YOU ARE A MICHIGAN RESIDENT: You may also obtain information about preventing identity theft and recommended next steps if you are the subject of identity theft from the Michigan State Police. You also have the right to obtain a police report if you are the subject of identity theft. The Michigan State Police can be reached at 7150 Harris Drive, Dimondale, MI 48821, 517-332-2521, https://www.michigan.gov/msp/0,4643,7-123-72297_41992_72431-128823--,00.html.

IF YOU ARE A MINNESOTA RESIDENT: You may also obtain information about avoiding identity theft from the Office of Minnesota Attorney General. This office can be reached at: Office of Minnesota Attorney General Keith Ellison, 445 Minnesota Street, Suite 1400, St. Paul,

MN 55101, (651) 296-3353 (Twin Cities Calling Area) or (800) 657-3787 (Outside the Twin Cities), <https://www.ag.state.mn.us/Consumer/IdentityTheft/Default.asp>.

IF YOU ARE A NEW JERSEY RESIDENT: You may also obtain information about avoiding identity theft from the Office of Consumer Protection. This office can be reached at: Office of Consumer Protection, Cyber Fraud Unit, P.O. Box 45025, Newark, New Jersey 07101, (973) 504-6200, <https://www.njconsumeraffairs.gov/ocp/Pages/cyberfraud.aspx>.

IF YOU ARE A NEW YORK RESIDENT: You may also obtain information about preventing identity theft from the New York Department of State's Division of Consumer Protection. This office can be reached at: New York State Division of Consumer Protection, 123 William Street, New York, NY 10038-3804, 1 (800) 697-1220, www.dos.ny.gov/consumerprotection.

IF YOU ARE A NORTH CAROLINA RESIDENT: You may also obtain information about avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at: 114 West Edenton Street, Raleigh, NC 27603, (919) 716-6400, or by its consumer hotline toll free within North Carolina at (919) 716-6000. <https://ncdoj.gov/protecting-consumers/>.

Sincerely,

BSH Home Appliances Corporation

«First_Name» «Last_Name»
«Address»
«City», «State» «Zip_Code»
«Email»

COMPLIMENTARY SERVICE OFFER: At our expense, BSH Home Appliances Corporation would like to offer you a free one-year subscription to Identity Guard® Essentials, an identity theft protection service. Identity Guard provides monitoring and protection and also alerts you of certain activities that could indicate potential identity theft. This program is provided by Intersections Inc. (NASDAQ: INTX), a leading provider of consumer and corporate identity risk management services.

Identity Guard® Essentials features include:

- Social Security Number Monitoring
- Online “Black Market” Monitoring
- Account Takeover Alerts
- \$1 Million Identity Theft Insurance*

- Lost Wallet Protection
- ID Verification™ Alerts
- ID Theft Victim Assistance
- ID Vault® Password Protection

If you wish to take advantage of this monitoring service, you must enroll by April 19, 2021.

ENROLLMENT PROCEDURE: To activate this coverage please visit the Web site listed below and enter the redemption code. The redemption code is required for enrollment, and can only be used one time by the individual addressed.

1. Website: www.identityguard.com/enroll
2. Redemption Code: «Redemption_Codes» and click “Submit”
3. Complete the Identity Guard Essentials enrollment form. To see additional product features, click “Service Details.”

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Redemption Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today. If you have any further questions regarding this incident, please contact BSH Home Appliances Corporation at the following email: data-response@bshg.com.

Sincerely,

BSH Home Appliances Corporation

*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.