LEWIS BRISBOIS BISGAARD & SMITH LLP

Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

April 6, 2020

VIA ELECTRONIC MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Wirepath Home Systems, LLC, which is the parent company of SunBriteTV, LLC ("SunBrite"), in connection with a recent data security incident described below.

I. Nature of Security Incident

SunBrite recently learned that its e-commerce website, sunbritetv.com, may have had its security compromised. Upon discovering this information, SunBrite immediately launched an investigation and engaged an independent digital forensics firm to determine what happened and what information may have been accessed. On March 20, 2020, the investigative firm reported that customers who made purchases through sunbritetv.com between October 13, 2019 and February 5, 2020 may have had their payment card data compromised, including name, address, card number, expiration date, and card verification value (CVV) number.

II. Number of New Hampshire Residents Affected

SunBrite has notified one (1) New Hampshire resident regarding this incident. Notification letters were mailed via first class U.S. mail on April 6, 2020. A sample copy of that notification letter is enclosed.

III. Actions Taken in Response to the Incident

SunBrite takes the security of its customers' information very seriously. As soon as SunBrite discovered the incident, it launched an investigation and took steps to stop any continued exposure

of sensitive information. It engaged a digital forensics firm to perform a comprehensive investigation and assist SunBrite in remediating any security issues related to its e-commerce site.

SunBrite is also providing affected consumers with complimentary credit monitoring, identity monitoring, identity theft expense reimbursement insurance; and fraud prevention and resolution support. It also notified the credit card brands of the compromise.

IV. Contact Information

SunBrite is dedicated to protecting its customers' personal information. If you have any questions or need additional information, please do not hesitate to contact me at (215) 977-4060 or Richard.Goldberg@lewisbrisbois.com.

Very truly yours,

/s/ Richard W. Goldberg

Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl. Sample Consumer Notification Letter

SunBriteTV®

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

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

Re: Notice of Data Security Incident

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

We are writing to inform you of a data security incident experienced by SunBriteTV, LLC ("SunBrite") that may have affected some of your personal information. The privacy and security of your information is extremely important to SunBrite. That is why we are writing to inform you of this incident, to offer you complimentary identity monitoring services, and to provide you with information relating to steps that can be taken to help safeguard your information.

What Happened? SunBrite recently learned that the security of its website, sunbritetv.com, may have been compromised. Upon discovering this incident, SunBrite immediately launched an investigation and engaged an independent digital forensics firm to determine what happened and what information may have been accessed. The investigation determined that customers who made purchases through sunbritetv.com between October 13, 2019 and February 5, 2020 may have had their payment card data compromised.

What Information Was Involved? The information involved in this incident may have included your name, address, payment card number, expiration date, and card verification value (CVV) number.

What Are We Doing? As soon as we discovered the incident, we launched an investigation and took steps to stop any continued exposure of information. We have also adopted enhanced security measures to prevent similar incidents in the future.

We are also providing you with information about steps that you can take to help safeguard your personal information. We have secured the services of Kroll to provide identity monitoring at no cost to you for eighteen months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What You Can Do: We strongly encourage you to activate the identity monitoring services we are offering through Kroll to help safeguard your personal information.

Visit **https://[IDMonitoringURL]** to activate and take advantage of your identity monitoring services.
*You have until **[Date]** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing the services provided to you is included with this letter.

We also recommend that you.

- Close any potentially affected financial accounts;
- Review your account statements for discrepancies, and report any discrepancies to your bank;
- Place a fraud alert on your credit report; and
- Place a security freeze on your credit file.

For More Information: Further information about how to help safeguard your personal information appears on the following page. If you have questions concerning this incident, please call 1-???-???-????, Monday through Friday from 7:00 a.m. to 4:30 p.m. Mountain Time excluding national holidays.

We take your trust in us seriously, and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Jonathan Johnson
Director of Retail and Consumer Sales
SunBriteTV, LLC

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend 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).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] 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.