POLSINELLI

Century Plaza Towers, 2049 Century Park East #2900, Los Angeles, CA 90067 • (310).559.1801

March 6, 2023

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

Attorney General John Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General Formella:

We represent Squishable.com, Inc. ("Squishable") in connection with a recent incident that may have resulted in the unauthorized interception of personal information for a number of Squishable customers. Squishable is reporting this incident pursuant to N.H. Rev. Stat. § 359-C:20.

This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Squishable is notifying you of this incident, Squishable does not waive any rights or defenses relating to the incident or this notice, including the applicability of New Hampshire jurisdiction over Squishable.

BACKGROUND OF THE INCIDENT

Squishable has learned that its website, Squishable.com, contained code that Squishable had not approved. Upon identifying the issue, Squishable removed the code from its website and launched an investigation in consultation with a leading forensic cybersecurity firm. Through its investigation, Squishable determined that the code allowed a third party to view and potentially capture information that was entered on the checkout page as customer made purchases on the website. The information that would have been entered on the checkout page included customer names, shipping and billing addressees, payment card information, and email addresses. Squishable determined that purchases made between May 26 and October 12, 2022, were subject to the code.

NOTICE OF THE INCIDENT

Squishable determined that the incident may have involved one hundred twenty-one (121) New Hampshire residents. Squishable mailed notifications letters to these individuals via First-Class

United States mail on March 2, 2023. Squishable has also arranged for a toll-free, dedicated call line to assist the notified customers with any questions they may have regarding the incident. Enclosed is a sample of the notification letter.

OTHER STEPS TAKEN RELATED TO THE INCIDENT

Upon learning of the incident, Squishable contained the incident by removing the unauthorized code. It also engaged a forensic security firm through counsel to investigate the incident and confirm the security of its systems. It has also notified federal law enforcement and is working with the payment card brands. Squishable is undertaking efforts to reduce the risk of a similar incident occurring in the future. Finally, as discussed above, Squishable is notifying the involved individuals, and has coordinated with payment card brands and federal law enforcement to keep them apprised of the situation.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Pavel (Pasha) A. Sternberg

Enclosure

228 Park Ave S. Suite 56124
New York City, NY 10003

<<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 BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Squishable.com, Inc. ("Squishable") is committed to the privacy of individuals and takes the protection of personal information that is entrusted to us seriously. Unfortunately, we are writing to make you aware of a recent data security incident that may have involved some of your personal information.

What Happened? On October 12, 2022, Squishable learned that its website contained code that Squishable had not approved. Upon identifying the issue, Squishable immediately launched an internal investigation and then enlisted the help of an outside third-party forensic firm to conduct a further investigation. The investigation determined that the code allowed a third party to view and potentially capture information that was entered on our checkout page as customers made purchases on the website between May 26 and October 12, 2022.

What Information Was Involved? Based on our investigation, information entered into the website's checkout page including your name, address, payment card information, and email address.

What We Are Doing. Upon learning of the situation, Squishable immediately launched an internal investigation and worked to remove the code from our website. We then engaged an external third-party forensic firm to investigate the incident and notified law enforcement. We are also working with the credit card brands to address the issue. Finally, we have updated our website's infrastructure to reduce the likelihood of this type of incident occurring in the future.

What You Can Do. It is generally recommended that you review your credit card statements and financial accounts for unauthorized activity. We also encourage you to review the information on steps you can take to protect yourself against possible identity theft or fraud, which is included in the enclosed *Additional Important Information* sheet.

For More Information. For further information and assistance, please call from 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays.

We value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience this incident might cause.

Sincerely,

Aaron Glazer, CEO
Squishable.com, Inc.
228 Park Avenue South Suite 56124
New York City, NY 10003

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, 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 a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report 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 new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

This notification was not delayed by law enforcement.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. 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 three (3) business days after receiving your request 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 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.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the District of Columbia Attorney General's office at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports without any charge

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected XX Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).