MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 25, 2021

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Sugarfina USA, LLC ("Sugarfina") located at 1700 E. Walnut Ave. 5th Floor, El Segundo, CA 90245 and write, on behalf of Sugarfina, to notify your Office of an incident that may affect the security of certain payment information of approximately one hundred fifty (150) New Hampshire residents. Preliminary notice of this event was submitted to your office on April 26, 2021. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Sugarfina does not waive any rights or defenses regarding the applicability of New Hampshire law, the New Hampshire data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On or around January 15, 2021, Sugarfina determined that it was the victim of a sophisticated cyber-attack and on March 25, 2021 determined that this attack that may have allowed unauthorized actors to gain access to certain customers' payment card information used to make purchases on www.sugarfina.com between November 1, 2019 and September 3, 2020. However, Sugarfina is unable to confirm whether the unauthorized actors actually accessed any payment cards during this time period. Sugarfina performed a comprehensive review of information stored on the impacted systems to determine what information was affected and to whom the information related. This included a manual review of its records to determine the identities and contact information for potentially impacted individuals, which was completed on April 21, 2021. During the investigation Sugarfina took steps to address the issue and to secure its website. Customers can safely and securely use their payment cards on Sugarfina's website. The investigation determined that the following types of information related to New Hampshire residents may have been

impacted: cardholders' name, address, credit card number, expiration date, CVV, and if provided, username and password.

Notice to New Hampshire Residents

On or around May 25, 2021, Sugarfina began providing written notice of this incident to potentially affected individuals, including approximately one hundred fifty (150) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of unusual activity related to its website, Sugarfina immediately launched an investigation to determine the nature and scope of this incident. As part of Sugarfina's ongoing commitment to the privacy of payment information in its care, Sugarfina is reviewing its existing policies and procedures and implementing additional safeguards to further secure the payment information. Sugarfina is also notifying relevant regulatory authorities of this event, as required by applicable law.

Sugarfina is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/laf
Enclosure

Exhibit A

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

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

<<b2b_text_1 (Header)>>

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

Sugarfina USA, LLC ("Sugarfina") writes to inform you of a recent event that may impact the privacy of some of your payment card information. We wanted to provide you with information about the event, our response, and steps you may wish to take to better protect against the possibility of identity theft and fraud.

What Happened? Sugarfina recently began investigating suspicious activity reported by a credit card company. Sugarfina immediately launched an investigation into the suspicious activity and performed a review of its website code. On or around January 15, 2021, the investigation determined that Sugarfina was the victim of a sophisticated cyber-attack and on March 25, 2021 determined that this attack may have allowed unauthorized actors to gain access to certain customers' payment card information used to make purchases on www.sugarfina.com between November 1, 2019 and September 3, 2020. However, Sugarfina is unable to confirm whether the unauthorized actors actually accessed any payment cards during this time period. Following these determinations, Sugarfina took steps to confirm the identity of the customers whose payment card information may have been used at www.sugarfina.com between November 1, 2019 and September 3, 2020. Sugarfina also took immediate steps to secure its website. You can safely and securely use your payment card on Sugarfina's website.

What Information Was Involved? Through the investigation, Sugarfina confirmed that malicious code on its website could have allowed unauthorized actors to gain access to customer payment card information from orders placed on www.sugarfina.com between November 1, 2019 and September 3, 2020. The information potentially impacted by this event includes the cardholder's name, billing address, credit card number, expiration date, CVV, and if provided, username and password.

What We Are Doing. Sugarfina takes this incident and the security of your information seriously. As part of our ongoing commitment to the privacy of personal information in our care, we are continuing to review our existing policies and procedures and to implement additional safeguards to further secure payment information. In addition to notifying potentially impacted individuals we are also notifying state regulators, as required.

What You Can Do. We encourage you to monitor your financial account statements and report any suspicious charges to the institution that issued your payment card. You can find the contact information on the back of your payment card. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Personal Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-???-???-???? Monday through Friday between 8:00 am to 5:30 pm Central Time. You may also write to Sugarfina at: 1700 E. Walnut Ave, 5th Floor, El Segundo, CA 90245.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Scott LaPorta

Chief Executive Officer
Sugarfina USA, LLC

Steps You Can Take to Help Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

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 two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report

with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 131 Rhode Island residents impacted by this incident.