CONSTANGY BROOKS, SMITH & PROPHETE LLP

September 1, 2023

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Notice of Third Party Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents Bennington Potters, a stoneware pottery maker, in connection with a third-party data security incident experienced by CommerceV3, a third-party vendor that provides an e-commerce platform utilized by Bennington Potters and other online retailers. This notice is being sent because information for New Hampshire residents may have been involved in the incident.

1. **Nature of the security incident.**

CommerceV3 learned that an unauthorized party obtained access to its systems between November 24, 2021, and December 14, 2022. Immediately upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to determine whether any cardholder data was accessed or acquired without authorization in connection with the incident. On May 3, 2023, after completion of the forensic investigation, CommerceV3 discovered that payment card information collected on Bennington Potters' behalf during online transactions was potentially accessed or acquired by an unauthorized party as a result of the incident. Bennington Potters received notice from CommerceV3 on June 30, 2023. Since that time, Bennington Potters have been working to gather contact information and take other steps needed to provide individual notification.

The potentially affected personal information for New Hampshire residents includes individuals'

for customers who purchased products through Bennington Potters' online store between November 24, 2021 and December 14, 2022.

2. **Number of New Hampshire residents affected.**

On August 31, 2023, Bennington Potters provided notification to 344 New Hampshire residents whose personal information may have been involved in the incident via email, Bennington Potters'

primary means of communicating with its customers. A sample copy of the notification is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Bennington Potters was informed of this incident, it contacted CommerceV3 for additional information related to the incident and gathered contact information to provide appropriate notification based on the information provided by CommerceV3. It is Bennington Potters' understanding that CommerceV3 also worked alongside the major card brands and banks during the forensic investigation, and that it has implemented additional security measures designed to protect the privacy of customer information.

Bennington Potters has established a toll-free call center through IDX to answer any questions about the incident and address related concerns. The call center is available from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

In addition, Bennington Potters is offering IDX Recovery Assistance at no cost to all individuals whose information may have been involved in this issue. With this service, IDX experts will assist individuals in resolving any unauthorized charges to their payment cards.

4. Contact information.

Bennington Potters remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

Aubrey Weaver
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Individual Notice

August 31, 2023

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Bennington Potters is writing to inform you of a data security incident at our third-party e-commerce platform, CommerceV3, that may have involved your payment card information. Please read this letter carefully as it contains information regarding the CommerceV3 incident, provides steps you can take to help protect your personal information, and provides you access to complimentary restoration assistance through IDX. As a result of this incident, we have partnered with IDX to provide you this notification.

What Happened: CommerceV3, a third-party vendor that provides an e-commerce platform utilized by Bennington Potters and other online retailers, learned that an unauthorized party obtained access to its systems between November 24, 2021, and December 14, 2022. Immediately upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to determine whether any cardholder data was accessed or acquired without authorization in connection with the incident. On May 3, 2023, after completion of the extensive forensic investigation, CommerceV3 discovered that payment card information collected on Bennington Potters' behalf during online transactions was potentially accessed or acquired by an unauthorized party as a result of the incident.

What Information Was Involved: CommerceV3's investigation revealed that this incident potentially involved for customers who purchased products through our online store between November 24, 2021, and December 14, 2022.

What We Are Doing: Bennington Potters received notice from CommerceV3 on June 30, 2023. Since that time, we have been working to gather contact information and take other steps needed to provide individual notification. We understand that CommerceV3 also worked alongside the major card brands and banks during the course of its forensic investigation, and that it has implemented additional security measures designed to protect the privacy of customer information.

What You Can Do: You can follow the recommendations included with this email to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

In addition, Bennington Potters has arranged to provide its customers complimentary restoration assistance through IDX, a data breach and recovery services expert. If you identify any payment card transactions that you do not understand or that look suspicious, or if you suspect that any fraudulent transactions have taken place, you can contact IDX's Certified Recovery Advocates at 1-888-657-7693, who will work on your behalf to help resolve these issues. IDX's Certified Recovery Advocates are available Monday through Friday from 9:00 am and 9:00 pm Eastern Time. Restoration assistance is available until August 30, 2024.

For More Information: If you have any questions regarding this email, we encourage you to contact our dedicated call center at between 9:00 am and 9:00 pm Eastern Time.

We take our customers' trust in Bennington Potters, and this matter, very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Bennington Potters, Inc.
324 County Street
Bennington, Vermont 05201

STEPS YOU CAN TAKE TO HELP 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 incidents 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 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.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 at least one 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 for up to one year at no cost. 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. 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 fraud alerts, security freezes, and 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.