LEWIS BRISBOIS BISGAARD & SMITH LLP

Shelly Hall
550 West Adams Street
Suite 300
Chicago, IL 60661
Shelly.Hall@lewisbrisbois.com
Direct: 312.463.3362

May 26, 2022

VIA Online Submission
Maine State Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, Maine 04330
Fax: 207-624-7730
E-mail: breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General:

Lewis Brisbois Bisgaard & Smith LLP represents 3T Brands, Inc. ("3T Brands"), headquartered in White Plains, New York, in connection with a recent data security incident that may have affected the information of certain Maine residents. This letter is sent under Me. Rev. Stat. Tit. 10 §§ 1346 – 1350-B.

1. NATURE OF THE SECURITY INCIDENT

3T Brands experienced a data security incident that prevented employees from accessing internal systems and data on August 11, 2021. 3T Brands immediately launched an investigation and engaged a digital forensics firm to help determine what happened and what information may have been accessed. 3T Brands also notified the FBI about the incident. Through its forensic investigation, 3T Brands identified unauthorized access from August 8-11, 2021 to certain data in its systems.

3T Brands also engaged independent experts to review of the data that could have potentially been accessed as a result of the incident, and, on May 2, 2022, determined that the information related to its employees, beneficiaries and other individuals, including the personal information of 9 Maine residents. To date, 3T Brands has no evidence that any of this information has been misused.

2. NUMBER OF MAINE RESIDENTS AFFECTED

3T Brands started notifying the 9 Maine residents of this data security incident via first class U.S. mail on May 26, 2022. A sample copy of the notification letter sent to the affected individuals is attached.

3. STEPS TAKEN RELATING TO THE INCIDENT

3T Brands has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to enhance the security of its digital environment. Furthermore, 3T Brands provided affected consumers with information about steps that they can take protect their personal information.

4. CONTACT INFORMATION

Please feel free to contact me at (312) 463-3362 or Shelly.Hall@lewisbrisbois.com if you have any further questions.

Respectfully,

/s/ Shelly Hall

Shelly Hall of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Individual Notification Letter

3T Brands, Inc.
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 26, 2022

Subject: Notice of Data <<variable data>>

Dear <<First Name>> <<Last Name>>:

At 3T Brands, Inc ("3T Brands") we are committed to protecting the confidentiality and security of the information we receive and maintain. We are writing to inform you of a recent data security incident we experienced that may have involved some of your information.

What Happened? We experienced a data security incident that prevented employees from accessing internal systems and data on August 11, 2021. Upon discovering this incident, we immediately launched an investigation and engaged a digital forensics firm to help determine what happened and what information may have been accessed. Through its investigation, we identified unauthorized access to certain data in its systems. We then engaged independent experts to analyze data to identify any personal information impacted and contact information for any affected individuals. We learned that your personal information may have been impacted in connection with the incident on May 2, 2022.

What Information Was Involved? The personal information potentially impacted by this incident included your name and your <<variable data>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We also notified law enforcement and implemented additional safeguards to help ensure the security of our network to reduce the risk of a similar event occurring in the future. In addition, we are offering you identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/ 24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What Can You Do? We encourage you to enroll in free identity protection services by calling 1-800-939-4170 or going to **https://app.idx.us/account-creation/protect** and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9am-9pm Eastern Time. Please note the deadline to enroll is August 26, 2022.

For More Information: Further information about how to protect your information appears on the following page. If you have questions concerning this incident, please contact 1-800-939-4170, Monday-Friday (excluding holidays), 9am-9pm Eastern Time. The security of your information is a top priority for 3T Brands. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you. Please call 1-800-939-4170 or go to **https://app.idx.us/account-creation/protect** for assistance or for any additional questions you may have.

Sincerely,
3T Brands, Inc.

ADDITIONAL 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You may also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the *Federal Trade Commission* is as follows: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338) - www.consumer.ftc.gov, www.ftc.gov/idtheft.

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:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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 fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps

the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. 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.

Additional Free Resources: You may contact 3T at 172 S Broadway, White Plains, NY 10605 or at 914-461-9877. 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, including the ones that follow for residents of those states.

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 2000; (202) 727-3400; oag@dc.gov

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: 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

Other Attorney Generals: Other Attorneys General can be located at: https://www.usa.gov/state-attorney-general.

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28Liberty Street, New York, NY 10005, 1-212-416-8433, https://ag.ny.gov/

Washington D.C.: Washington D.C. Attorney General can be reached at: 441 4th Street, NW Washington, DC 20001, 1-202-727-3400, oag.dc.gov