McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Janet

McGUIREWOODS

RECEIVED
JUL 14 2023
CONSUMER PROTECTION

July 13, 2023

VIA FEDEX
The Honorable John Formella
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice of Data Breach

Dear Attorney General Formella:

I am writing on behalf of Best Friends Pet Care, Inc. ("Best Friends" or the "Company"), with a headquarters located at 535 Connecticut Ave, Suite 305, Norwalk, CT 06854, to provide a report of a recent data breach. Best Friends provides pet care facilities, boarding, grooming, daycare, training, veterinary care, and pet products.

On April 19, 2023, Best Friends' information technology team discovered that a Company email account had been compromised and accessed by an unauthorized individual beginning on April 17, 2023. While Best Friends has implemented multifactor authentication ("MFA") on all of its email accounts, unbeknownst to Best Friends, the MFA for this particular email account had been disabled. Best Friends immediately engaged a professional forensic investigator to assess the incident. On June 9, 2023, the forensic investigator provided preliminary data regarding the information involved in the incident. So far, there is no evidence that any personal information was exfiltrated or otherwise removed from Best Friends' servers, but it does appear that the unauthorized individual had access to it. Best Friends has no indications that any of the data has been used for fraudulent purposes, nor are we aware of any resulting identity theft, fraud, or financial losses. Nevertheless, out of an abundance of caution, the Company is notifying the individuals whose information was located in the impacted accounts that their personal information may have been exposed.

While Best Friends learned of the breach on April 19, 2023, the nature of the data that appeared to be involved was such that addresses for the impacted individuals were not all immediately present. As such, Best Friends and its vendor have been working, and continue to work, together to identify the contact information for the impacted individuals so that Best Friends can notify the individuals of the incident. The first batch of this information was

completed on July 6, 2023. This batch of data revealed that four (4) New Hampshire residents had information involved in the breach. If the data still being analyzed reveals additional New Hampshire residents, we will provide a supplemental notice to your office.

The personal information that may have been accessed in Best Friend's systems includes certain New Hampshire residents'

Notices are being sent to the impacted individuals four individuals noted above tomorrow, July 14, 2023.

Best Friends contained the incident and immediately commenced an investigation. Best Friends also enhanced its MFA protections, implemented a new spam detection platform, moved from an individual IT manager to a fully-outsourced, professional, end-to-end technology service company, and undertook a full forensics investigation of the incident. In addition, Best Friends is offering each impacted New Hampshire resident a complimentary membership in Kroll's Credit Monitoring, Fraud Consultation, and Identity Theft Restoration services.

A copy of the template form of the notification letter that is being sent to the affected New Hampshire residents on July 14, 2023 is included with this notice as Exhibit A. As you will see, among other things, the letter (i) describes various steps that affected individuals can take to protect themselves, (ii) provides contact information for consumer reporting agencies and relevant governmental agencies, and (iii) provides information about enrolling in 12 months of credit monitoring services, which the Company is offering to the affected individual at no cost. An appendix is also attached with the letter as Exhibit B, which will serve as a key for your reference to the "text" field in the letter, which is a variable depending on the particular personal information involved.

If you have questions about this incident, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Janet P. Peyton

Enclosure: Template Notification Letter w/Appendix

EXHIBIT A

Best Friends
PET HOTEL

<<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>>,

I am writing to you on behalf of Best Friends Pet Care, Inc. ("Best Friends" or the "Company") with important information about a data security incident that occurred at Best Friends. Best Friends takes the protection and proper use of your personal information very seriously. We are, therefore, contacting you to explain the incident and provide you information about security measures you can take to help protect yourself and your personal information.

What Happened:

On April 19, 2023, Best Friends' information technology team discovered that a Company email account had been compromised and accessed by an unauthorized individual beginning on April 17, 2023. Best Friends immediately engaged a professional forensic investigator to assess the incident. On June 9, 2023, the forensic investigator provided preliminary data regarding the information involved in the incident and it was at that point that we learned that your information was involved. <<b2b_text_1 (RI Insert)>> This notice was not delayed as the result of a law enforcement investigation.

What Information Was Involved:

So far, there is no evidence that any personal information was exfiltrated or otherwise removed from Best Friends' servers, but it does appear that the unauthorized individual had access to it. Best Friends has no indications that any of the data has been used for fraudulent purposes, nor are we aware of any resulting identity theft, fraud, or financial losses. Personal information potentially disclosed as a result of this incident included your: <<b2b_text_2 (data elements)>>. Again, while we do not know whether your personal information was in fact accessed or used for any unauthorized purpose, we are sending you this notice as a precautionary action.

What We Are Doing:

We have taken actions to mitigate the incident, including successfully locking out the unauthorized user from the Company's system, enhancing the multifactor authentication protections used to keep email accounts secure, implementing a new spam detection platform, and undertaking a full forensic investigation of the incident.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for . 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.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

To enhance our security going forward, Best Friends has hired a professional third-party IT and cybersecurity firm to oversee our needs, confirmed that MFA is enabled for all of our email accounts, and added improved spam filters to our email servers. These changes are designed to enhance our data security and reduce the likelihood of future incidents like this one.

What You Can Do:

Please review the "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also report any suspected incident of identity theft to law enforcement, and you can obtain a copy of any resulting police report. If you do suspect that you have been the victim of identity theft, you should also notify your state Attorney General and the FTC.

For More information:

If you have questions, please call **TFN,** Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you and the enhancements to our security protocols demonstrate our continued commitment to your security and satisfaction.

We sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,

Marc Leahy
Chief Financial Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: You may contact the RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400; http://www.riag.ri.gov/ConsumerProtection/About.php#

ChexSystems

If your bank account information was involved in the incident, you may place a security alert and/or security freeze with ChexSystems by visiting https://www.chexsystems.com or calling

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.