LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
One PPG Place, 28th Floor
Pittsburgh, Pennsylvania 15222
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

August 16, 2021

VIA Online Portal

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notification of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents PetVet Care Centers ("PetVet") in connection with a recent data security incident which impacted one of their veterinary hospitals, Eastgate Animal Hospital, described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute.

1. Nature of the Security Incident

Eastgate Animal Hospital is a veterinary hospital located in Cincinnati, Ohio.

On July 3, 2021, PetVet became aware of suspicious activity in their computer environment at one of their veterinary hospitals, Eastgate Animal Hospital. Immediately upon discovery, PetVet took steps to secure its digital environment. Additionally, PetVet retained incident response counsel to assist with its response efforts and conducted an internal investigation to determine the source and scope of the incident. The investigation revealed that an unknown actor gained access to the Eastgate Animal Hospital Environment and may have been able to obtain information therein without authorization. PetVet has identified and remediated the initial point of intrusion for the unknown actor.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately two Maine residents. The information involved may include date of birth, Social Security number, Driver's License number, or credit card information.

Affected individuals will receive a letter notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The notification letters were sent via USPS First Class Mail on August 17, 2021.

3. Measures Taken to Address the Incident

In response to the incident, PetVet launched an internal forensics investigation to determine the source and scope of the compromise. PetVet also has implemented additional safeguards, such as enhanced employee training, rebuilding the server, upgrading their firewall, deploying an endpoint detection software which monitors the network environment, to help prevent a similar incident from occurring in the future.

As discussed above, PetVet is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

PetVet is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Lauren Godfrey at Lauren.Godfrey@lewisbrisbois.com.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

LDG: sgg
Encl.: Sample Notification Letter

<<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 Security incident

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

Eastgate Animal Hospital ("Eastgate") is writing to notify you of a recent data security incident that may have involved your personal information. Eastgate takes the privacy and security of your personal information very seriously. We want to inform you of this incident and about steps you can take to help protect your personal information and offer you complimentary identity monitoring services.

What Happened? On or about July 3, 2021, Eastgate became aware of unusual activity affecting Eastgate's computers. Eastgate information technology personnel immediately launched an investigation which determined that we had experienced a malware attack and that an unknown actor may have gained access to and obtained data from the Eastgate network without authorization. On July 26, 2021, we determined that some of your personal information may have been involved in the incident. This is why we are informing you of the incident and providing you with access to complementary identity monitoring services from Kroll. We have no information at this time that your information has been misused.

What Information Was Involved? The following information may have been impacted in connection with this incident: your <<b2b_text_1(Impacted Data)>>.

What We Are Doing. After discovering the incident, Eastgate implemented additional security features to reduce the risk of a similar incident occurring in the future. We are cooperating with the Federal Bureau of Investigation and will provide whatever assistance is necessary to attempt to hold the perpetrators of this incident accountable, if possible. We are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary identity monitoring services for twelve months at no cost to you through Kroll. 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 12 months of Single Bureau Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Additional information describing your services is included with this letter.

What You Can Do. Please review this letter carefully, along with the enclosed guidance providing additional steps you can take to help protect your information. We also encourage you to activate the identity monitoring services we are offering at no cost to you.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **November 18, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call our dedicated call center at 1-???-???_???? from 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major US holidays. Kroll representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Eastgate Animal Hospital

Steps You Can Take to Help Protect Your Personal 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 incidence 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 can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	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	**North Carolina Attorney General**	**Ohio Attorney General**
600 Pennsylvania Ave, NW	9001 Mail Service Center	30 E. Broad St,
Washington, DC 20580	Raleigh, NC 27699	14th Floor
consumer.ftc.gov, and	ncdoj.gov	Columbus, Ohio 43215
www.ftc.gov/idtheft	1-877-566-7226	www.ohioattorneygeneral.gov/
1-877-438-4338		1-855-224-6446

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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.