17018

PETERSON & SMITH Equine Hospital
Tradition • Leadership • Excellence

March 25, 2020

«Employee_First_Name» «Employee_Last_Name_and_Suffix»
«MAILING_ADDRESS»
«Employee_Address_2»
«Employee_City», «Employee_State_Prov» «Employee_ZipPostal_Code»

NOTICE OF UNAUTHORIZED SYSTEMS ACCESS

Dear «Employee_First_Name»:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

On January 17, 2020, at approximately 10:33 AM, Peterson & Smith Equine Hospital, LLC ("Peterson & Smith") it appears that there was an unauthorized access of Peterson & Smith's computer systems. Peterson & Smith's IT team became aware of a potential issue approximately thirty minutes later. Upon discovering the unauthorized access, Peterson & Smith acted quickly to minimize any potential risk by removing the associated technology from the system and commencing a thorough review. A review of Peterson & Smith's systems, conducted by a forensic investigator hired by Peterson & Smith, revealed that the attack was malware named 'Ryuk'. The forensic investigation revealed that Ryuk was active on the 'Q' drive, where some personal information on Peterson & Smith's employees is kept. There is no confirmation, or even any evidence, that any personal information was accessed. However, because the Ryuk malware is capable of copying information from files, it is possible that personal information of Peterson & Smith's employees was accessed. It appears that this attack was directed at Peterson & Smith itself and not to capture customer information.

WHAT INFORMATION WAS INVOLVED?

Peterson & Smith has been unable to confirm that any personal information of its employees was accessed. However, the files that may have been accessed and copied may have included personal information such as the name, address and social security numbers of employees of Peterson & Smith.

WHAT WE ARE DOING

Peterson & Smith has hired a forensic examiner and conducted a thorough review of the potentially affected computer systems and does not believe that there are any significant risks at this time. However, out of an abundance of caution, Peterson & Smith is taking additional steps to improve our security measures, such as:

- notifying employees whose information could have been compromised; and
- forcing password changes in various departments sooner than regularly scheduled.

Peterson & Smith will continue working to ensure the incident is properly addressed and will take any further actions as needed.

Peterson & Smith values your privacy and deeply regrets this event occurred.

WHAT YOU CAN DO

Please review the attachments to this letter (Best Practices to Protect Personal Information) for information on steps you can take to protect your information.

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code «Activation_Code» and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code 698861 and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **June 30, 2020**. Due to privacy laws, we cannot register you directly. Please note that credit

monitoring services might not be available for individuals who do not have a credit file with TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

FOR MORE INFORMATION

For further information and assistance, please contact Kalee George at (352) 237-6151 or Kgeorge@petersonsmith.com.

Sincerely,

Philip M Matthews
Peterson & Smith Equine Hospital

BEST PRACTICES TO PROTECT PERSONAL INFORMATION

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

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 access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **Take Advantage of Additional Free Resources on Identity Theft**

Review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

OTHER IMPORTANT INFORMATION

- **Place a Fraud Alert on Your Credit Report**

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 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. 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**

In some states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.