September 17, 2020

Eva J. Pulliam
Partner
202.857.6323 DIRECT
202.857.6395 FAX
eva.pulliam@arentfox.com

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504
SecurityBreach@atg.wa.gov

RE: INCIDENT NOTIFICATION

Dear Sir or Madam:

We are writing on behalf of Ponti Veterinary Hospital ("Ponti") and VCA Animal Hospitals ("VCA") to inform you of a ransomware incident involving Washington residents. At the outset, we note that fewer than 500 Washington state residents had data impacted that triggers the definition of a "data breach" under Washington law. However, given the large number of Washington residents for whom we have provided a courtesy notice paired with those whose data triggered notification requirements, we feel it is appropriate to notify the Attorney General.

As background, Ponti is a local veterinary hospital and was established in 1977 in Otis Orchards, Washington for the treatment and care of a diverse population of animals and wildlife in the greater Spokane and Idaho Panhandle areas. On August 18, 2020, VCA assumed operations of Ponti and, on that same day, became aware of recent attacks on Ponti's computer systems that occurred under Ponti's management. VCA immediately and diligently began an investigation into these attacks. In its investigations, it found that Ponti's computer systems were encrypted on or around August 14, 2020 and August 17, 2020. These attacks prevented Ponti from accessing customer and employee data.

At this time, we know that Ponti's HR systems were impacted, thus we are providing notice and credit monitoring to employees. While a small number of consumers had payment information impacted, we did not locate evidence that the majority of consumers had sensitive information exposed by the incident. In total, we are providing 135 breach notification letters to Washington state residents (employees and a small number of consumers) and 3,383 courtesy notifications to those for whom we do not believe sensitive information was impacted during the incident. These notifications were made on September 17, 2020.

We are only able to confirm that the information was encrypted so IT systems were inaccessible for a short period of time by Ponti. We have no evidence that personal information was acquired by the threat actor, and all systems are now fully recovered.

After conducting a full investigation of the incident with the support of cybersecurity and privacy experts including outside firms, we have put in place several additional security controls to prevent this from happening again. This includes the deployment of next generation anti-malware software, updated firewall controls, rebuilt systems, and patched and updated software. We are actively monitoring to protect against further incidents.

Sample copies of the notification letters are enclosed. Please do not hesitate to contact me if you have any questions or require additional information.

Respectfully submitted,

Eva J. Pulliam
Partner

Attachments

VCA Ponti Animal Hospital

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 17, 2020

F7985-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L01 PONTI ASSOCIATE
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Data Incident Notification

Dear Ponti Associate:

We're writing to you as a valued associate or former associate of Ponti Veterinary Hospital ("Ponti") to inform you of a cybersecurity incident that affected our hospital and possibly your associate data. We are unaware of any actual access to, acquisition of, or misuse of your information; we are providing notice to you about this incident because we care about your privacy.

What Happened?	Ponti's technology systems, including its systems holding customer and associate data, were subject to two cyberattacks on or around August 14, 2020 and August 17, 2020. VCA Animal Hospitals became aware of the attacks on August 18, 2020, the day that it assumed operations of Ponti. As part of the attacks, Ponti's computer systems were encrypted, preventing Ponti from accessing customer and associate data.
What Information Was Involved?	At this time, we know that Ponti's affected systems included personal information such as employee contact information, birth date, address, personal email address, social security number, pay rates, performance records, tax and/or claim information, and/or direct deposit information (if participating in direct deposit). We are only able to confirm that the information was encrypted so that it could not be accessed for a short period of time by Ponti. We have no evidence that your personal information was acquired, and Ponti's systems have fully recovered.

What are We Doing?	Protecting the privacy and security of your data is of critical importance to Ponti. After conducting a full investigation of the incident with the support of cybersecurity and privacy experts, we have put in place additional security controls to protect against future attacks and we are actively monitoring to protect against further incidents. Though we have no basis to believe that any of your personal data was taken, Ponti is informing you of this incident because we respect your privacy.
What You Can Do.	As a precautionary measure, we encourage you to remain alert to monitor for phishing attacks or other misuse of your personal information. Further, while we have no reason to believe that sensitive financial information was exposed, it is always good practice to monitor your account statements and credit reports to guard against fraud and identity theft. For your convenience, we have provided contact information for the three major credit reporting agencies below. These credit reporting agencies provide a free copy of your credit report, at your request, once every 12 months: Equifax (800) 685-1111 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) 916-8800 www.transunion.com P.O. Box 2000 Chester, PA 19016 Additionally, to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for one year. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that Identity Restoration is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

	While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary one year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below: • Ensure that you enroll by December 31, 2020 (Your code will not work after this date.) • Visit the Experian IdentityWorks website to enroll: [redacted] • Provide your activation code: ABCDEFGHI If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by December 31, 2020. Be prepared to provide [redacted] as proof of eligibility for the Identity Restoration services by Experian.
For More Information.	For more information, call [redacted]. You may also email us at [redacted]. For more information, you may also contact [redacted] with "Ponti" in the subject line.

Sincerely,

Todd Lavender, DVM

President, VCA Animal Hospitals & Petcare Services

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

VCA Ponti Animal Hospital

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 17, 2020

F7985-L02-0000002 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L02 PONTI CUSTOMER CM
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Data Incident Notification

Dear Ponti Customer:

We're writing to you as a valued customer of Ponti Veterinary Hospital ("Ponti") to inform you of a cybersecurity incident that affected our hospital and possibly your customer data. We are unaware of any actual access to, acquisition of, or misuse of your information; we are providing notice to you about this incident because we respect your privacy.

What Happened?	Ponti's technology systems, including its systems holding customer and associate data, were subject to two cyberattacks on or around August 14, 2020 and August 17, 2020. VCA Animal Hospitals became aware of the attacks on August 18, 2020, the day that it assumed operations of Ponti. As part of the attacks, Ponti's computer systems were encrypted, preventing Ponti from accessing customer and associate data.
What Information Was Involved?	At this time, we know that Ponti's affected systems included financial information, such as CareCredit or credit card information. We are only able to confirm that the information was encrypted so that it could not be accessed for a short period of time by Ponti. We have no evidence that your personal information was acquired, and Ponti's systems have fully recovered.
What are We Doing?	Protecting the privacy and security of your data is of critical importance to Ponti. After conducting a full investigation of the incident with the support of cybersecurity and privacy experts, we have put in place additional security controls to protect against future attacks and we are actively monitoring to protect against further incidents. Though we have no basis to believe that any of your personal data was taken, Ponti is informing you of this incident because we respect your privacy.

What You Can Do.	As a precautionary measure, we encourage you to remain alert to monitor for phishing attacks or other misuse of your personal information. Further, while we have no reason to believe that sensitive financial information was exposed, it is always good practice to monitor your account statements and credit reports to guard against fraud and identity theft. For your convenience, we have provided contact information for the three major credit reporting agencies below. These credit reporting agencies provide a free copy of your credit report, at your request, once every 12 months: Equifax (800) 685-1111 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) 916-8800 www.transunion.com P.O. Box 2000 Chester, PA 19016 You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the U.S. Federal Trade Commission ("FTC"). The FTC provides further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580; by phone at 1-877-ID-THEFT (877-438-4338); or online at www.consumer.gov/idtheft. Additionally, to help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for one year. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

	Please note that Identity Restoration is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary one year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below: • Ensure that you enroll by December 31, 2020 (Your code will not work after this date.) • Visit the Experian IdentityWorks website to enroll: [redacted] • Provide your activation code: ABCDEFGHI If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by December 31, 2020. Be prepared to provide [redacted] as proof of eligibility for the Identity Restoration services by Experian.
For More Information.	For more information, call [redacted]. You may also email us at [redacted]

Sincerely,

Todd Lavender, DVM

President, VCA Animal Hospitals & Petcare Services

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

VCA Ponti Animal Hospital

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 17, 2020

F7985-L03-0000003 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L03 PONTI CUSTOMER NO CM
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Data Incident Notification

Dear Ponti Customer:

We're writing to you as a valued customer of Ponti Veterinary Hospital ("Ponti") to inform you of a cybersecurity incident that affected our hospital and possibly your customer data. We are unaware of any actual access to, acquisition of, or misuse of your information; we are providing notice to you about this incident because we respect your privacy.

What Happened?	Ponti's technology systems, including its systems holding customer and associate data, were subject to two cyberattacks on or around August 14, 2020 and August 17, 2020. VCA Animal Hospitals became aware of the attacks on August 18, 2020, the day that it assumed operations of Ponti. As part of the attacks, Ponti's computer systems were encrypted, preventing Ponti from accessing customer and associate data.
What Information Was Involved?	We are only able to confirm that the information was encrypted so that it could not be accessed for a short period of time by Ponti. We have no evidence that your personal information was acquired, and Ponti's systems have fully recovered.
What are We Doing?	Protecting the privacy and security of your data is of critical importance to Ponti. After conducting a full investigation of the incident with the support of cybersecurity and privacy experts, we have put in place additional security controls to protect against future attacks and we are actively monitoring to protect against further incidents. Though we have no basis to believe that any of your personal data was taken, Ponti is informing you of this incident because we respect your privacy.

What You Can Do.	As a precautionary measure, we encourage you to remain alert to monitor for phishing attacks or other misuse of your personal information. Further, while we have no reason to believe that sensitive financial information was exposed, it is always good practice to monitor your account statements and credit reports to guard against fraud and identity theft. For your convenience, we have provided contact information for the three major credit reporting agencies below. These credit reporting agencies provide a free copy of your credit report, at your request, once every 12 months: Equifax (800) 685-1111 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) 916-8800 www.transunion.com P.O. Box 2000 Chester, PA 19016 You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the U.S. Federal Trade Commission ("FTC"). The FTC provides further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580; by phone at 1-877-ID-THEFT (877-438-4338); or online at www.consumer.gov/idtheft.
For More Information.	For more information, call [redacted] and be prepared to reference [redacted]. You may also email us at [redacted]

Sincerely,

Todd

Todd Lavender, DVM

President, VCA Animal Hospitals & Petcare Services