



Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
Telephone: 503.312.6251
Email: dmaddux@constangy.com

May 19, 2023

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202
Email: idtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Davis Reeder Hall DVM, PLC dba Town and Country Animal Hospital & Columbia Pike Animal Hospital and Emergency Center (“T&CAH”), an animal hospital located in Fairfax, Virginia, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On March 28, 2023, T&CAH learned that certain employees discovered fraudulent tax forms filed on their behalf. In response, T&CAH immediately retained independent cybersecurity experts to conduct a forensic investigation to determine whether any personal information may have been accessed or acquired.

Based on that investigation, on April 19, 2023, T&CAH learned that an unauthorized actor accessed a single employee account and acquired an administrative file containing employee personal information. T&CAH then worked diligently to identify individuals whose information may have been impacted, as well as current address information to effectuate notification. That process was completed on April 27, 2023.

T&CAH is notifying all potentially impacted individuals of the incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

2. Number of Affected Maryland Residents & Information Involved

This incident involved the personal information for twenty-six (26) Maryland residents. The information involved in the incident includes Maryland resident's name and Social Security number.

3. Notification of Affected Individuals

On May 19, 2023, notification letters were mailed to affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose personal information was affected by this event, including 24 months of credit monitoring, and fully managed identity theft recovery services. Those services are offered through Experian, a leader in risk mitigation and response specializing in fraud assistance and remediation services. Experian will also support a call center for 90 days to answer questions and assist with enrollment. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken to Address the Incident

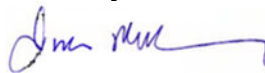
In response to the incident, T&CAH retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. T&CAH also implemented additional security measures to further harden its email environment in an effort to prevent a similar event from occurring in the future. Additionally, T&CAH has reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, T&CAH is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

4. Contact Information

T&CAH remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at DMaddux@Constangy.com or 503.312.6251.

Sincerely,

A handwritten signature in blue ink, appearing to read "Donna Maddux", with a long horizontal flourish extending to the right.

Donna Maddux of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter



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

J4534-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 CONSUMER
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



May 19, 2023

Subject: Notice of Data Security Incident

Dear Sample A. Sample:

We are writing to inform you about a recent data security incident experienced by Davis Reeder Hall DVM, PLC dba Town and Country Animal Hospital & Columbia Pike Animal Hospital and Emergency Center (“T&CAH”) that involved your personal information. Please read this letter carefully. It contains important details about the incident and resources you may utilize to help protect your personal information.

What Happened? On March 28, 2023, we were made aware that some of our employees discovered fraudulent tax forms filed on their behalf. With the assistance of independent cybersecurity experts, we immediately initiated an investigation. Based on that investigation, on April 19, 2023, we learned that an unknown actor acquired an administrative file which contained employee personal information. We then undertook a comprehensive review of the impacted data to determine the scope of the personal information involved. That process concluded on April 27, 2023, and we identified that your information was included in the impacted administrative file.

What Information Was Involved? The information that may have been involved in this incident includes your name, as well as your Social Security number.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. As part of the response process, we implemented additional measures to reduce the risk of a similar incident occurring in the future. T&CAH also reported this incident to federal law enforcement and will assist with any related investigation. In addition, we are providing additional steps you can take to help protect your information.

Finally, we are offering you the ability to enroll in complimentary identity protection services through Experian IdentityWorks—a data breach and recovery services expert. These services include 24 months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** August 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/plus>
- Provide your **activation code**: ABCDEFGHI

¹ To receive credit monitoring 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.



If you have questions about the product or need assistance with enrolling, please contact Experian's customer care team at (833) 420-2864 by August 31, 2023. Please be prepared to provide engagement number B091252 as proof of eligibility.

What Can You Do? We recommend that you review the guidance included with this letter about how to protect your information. We also encourage you to enroll in the complimentary identity protection services being offered to you through Experian IdentityWorks by using the activation code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call Experian at (833) 420-2864 Monday through Friday from 6 am – 8 pm Pacific, or Saturday and Sunday from 8 am – 5 pm Pacific (excluding major U.S. holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Terry Lyn Bishop

Terry Lyn Bishop
Chief Operating Officer
Town & Country Animal Hospital

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 should 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 proof. 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. 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. 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 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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; [202-727-3400](tel:202-727-3400); oag@dc.gov

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

ADDITIONAL DETAILS REGARDING YOUR 24 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.
- Internet Surveillance: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- 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 As-surant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.