

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

March 30, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Anthony Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: American Paint Horse Association – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents American Paint Horse Association (“APHA”). I am writing to provide notification of an incident at APHA that may affect the security of personal information of approximately three (3) Maryland residents. APHA’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, APHA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On February 27, 2023, APHA prepared and mailed 1099-Miscellaneous forms to certain members containing names, addresses, and Social Security numbers. On or about March 1, 2023, APHA learned that some of their members may have had their names, addresses, and Social Security numbers inadvertently viewable in the address window of the envelope in which their 1099 Miscellaneous was mailed. When preparing the mailing, SSNs were not viewable but during the mailing process, contents may have shuffled and Social Security numbers may have been potentially viewable by unauthorized parties. APHA mailed the forms to the appropriate address on file and, to date, is not aware of any instances of identity fraud as a result of the inadvertent disclosure.

Upon learning of this issue, APHA immediately commenced an internal investigation and promptly notified potentially affected individuals. APHA wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. APHA is providing the affected residents with written notification of this incident commencing on or about March 31, 2023 in substantially the same form as the letter attached hereto. APHA is offering residents complimentary one-year membership with a credit monitoring service. APHA will advise the affected residents to always

March 30, 2023

Page 2

remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. APHA will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At APHA, protecting the privacy of personal information is a top priority. APHA is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. APHA continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Very truly yours,



Dominic A. Paluzzi

Encl.

American Paint Horse Association
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07307

A M E R I C A N
P A I N T
H O R S E
A S S O C I A T I O N

March 31, 2023

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to the American Paint Horse Association (APHA). We are writing to provide you with important information about a recent incident which involves the security of some of your personal information that was supplied to us. We want to provide you with information regarding the incident and explain the services we are making available to help safeguard against identity fraud. We also are providing additional steps you can take to further protect your information.

What Happened?

On February 27, 2023, we prepared and mailed 1099-Miscellaneous forms to certain members containing names, addresses, and Social Security numbers. On March 1, 2023, we learned that some information may have been inadvertently viewable in the address window of the envelope in which the 1099 Miscellaneous was mailed. When preparing the mailing Social Security numbers were not viewable, but during the mailing process contents may have shuffled and your Social Security number may have been potentially viewable by unauthorized parties. Upon learning of the issue, we commenced a prompt and thorough investigation.

What Information Was Involved?

The information that was potentially viewable in the address window included your name, address, and Social Security number contained on your 1099 Miscellaneous.

What We Are Doing.

We have no reason to suspect that any of the information in the address window has been or will be acquired or misused by an unauthorized individual. 1099 Miscellaneous were mailed to the correct recipient. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What You Can Do.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. For more information on

identity theft prevention and instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

If you have any further questions regarding this incident, representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code provided in this letter.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,

A handwritten signature in black ink, appearing to read "Billy Smith". The signature is fluid and cursive, with a large initial "B" and "S".

Billy Smith, Executive Director
American Paint Horse Association

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12 months Credit Monitoring

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/paintedhorse>** and follow the instructions provided. When prompted please provide the following unique code to receive services: XXXXXXXXXX

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the other credit bureaus.

Equifax

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion LLC

P.O. Box 6790

Fullerton, PA 92834-6790

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(800) 349-9960

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000

Chester, PA 19016

<http://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Reporting Identity Fraud to the IRS.

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police or law enforcement department.

You may also request an Identity Protection PIN from the IRS. The Identity Protection PIN is a six-digit number the IRS assigns to an individual to help prevent misuse of their Social Security number or Individual Taxpayer Identification Number on federal tax returns. The IRS may automatically assign an Identity Protection PIN if you are a confirmed victim of tax-related identity theft. Otherwise, you can request an Identity Protection PIN at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>.

6. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount. The Social Security Administration has published Identity Theft and Your Social Security Number at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

7. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392