

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

April 24, 2023

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

Brian E. Frosh
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: DignityUSA – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents DignityUSA (“Dignity”). I am writing to provide notification of an incident at Dignity that may affect the security of personal information of approximately one (1) Maryland resident. Dignity’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, Dignity does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or around March 7, 2023 Dignity detected suspicious activity impacting an employee’s email account that was later determined to be an email compromise. Upon learning of this issue, Dignity contained the threat by disabling all unauthorized access to its email environment and resetting passwords. Dignity immediately started a thorough investigation of the matter and has been working with external cybersecurity professionals experienced in handling these types of incidents. Dignity discovered on April 10, 2023 that an unauthorized individual potentially accessed or viewed emails between February 4, 2023 and March 7, 2023 that may have contained personal information such as a full name along with a Credit / Debit Card Number, Expiration Date/CVV/Security Code, Passport Number, and Social Security number.

Dignity has no reason to believe any personal information will be misused as a result of this incident. Nevertheless, out of an abundance of caution, Dignity wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Dignity is providing the affected resident with written notification of this incident commencing on or about April 24, 2023 in substantially the same form

as the letter attached hereto. Dignity is offering the affected resident a complimentary one-year membership with a credit monitoring service. Dignity is advising the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Dignity is advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Should you have any questions regarding this notification, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock". The signature is fluid and cursive, with a large initial "S" and a distinct "P".

Spencer S. Pollock

Encl.



P.O. Box 1228
Dunkirk, MD 20754

[REDACTED]

Dear [REDACTED]

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to DignityUSA (“Dignity”). We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

On or around March 7, 2023 Dignity detected suspicious activity impacting an employee’s email account that was later determined to be an email compromise.

What We Are Doing

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our email environment and resetting passwords. We immediately started a thorough investigation of the matter and have been working with external cybersecurity professionals experienced in handling these types of incidents. We discovered on April 10, 2023 that an unauthorized individual potentially accessed or viewed emails between February 4, 2023 and March 7, 2023 that may have contained some of your personal information.

What Information Was Involved

The potentially accessed information included your full name along with your [REDACTED] **As of now, we have no evidence indicating any of your information has been used for identity theft or financial fraud.**

What You Can Do

Out of an abundance of caution, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by TransUnion, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

This letter also provides other precautionary measures you can take to protect your information from potential misuse, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports on a regular basis for fraudulent or irregular activity.

For More Information

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 personal information.

If you have any further questions regarding this incident, please call [REDACTED]

Sincerely,

DignityUSA

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one (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 others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<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

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://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 reporting 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.

3. 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.

4. 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 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.

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.

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: 888-743-0023