McDonald Hopkins
A business advisory and advocacy law firm®

1820 Lancaster Street
Suites 208 & 209
Baltimore, MD 21231

P: 1.410.917.5189

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

January 31, 2025

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

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

Re: VLP Copenhaver Espino – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents VLP Copenhaver Espino. I am writing to provide notification of an incident at VLP Copenhaver Espino that may affect the security of personal information of one (1) Maryland resident. VLP Copenhaver Espino will supplement this notification with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, VLP Copenhaver Espino does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about September 18, 2024, VLP Copenhaver Espino detected unauthorized access to their network. Upon learning of this issue, VLP Copenhaver Espino immediately secured the environment and commenced a prompt and thorough investigation. As part of its investigation, VLP Copenhaver Espino worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and document review, VLP Copenhaver Espino discovered on January 16, 2025, that between May 27, 2024 and September 18, 2024, certain impacted files containing personal information may have been accessed and/or acquired by an unauthorized individual. Further, on January 27, 2025, VLP Copenhaver Espino located the most recent contact information for the affected residents. The personal information contained within the impacted data included first and last name and Social Security number.

VLP Copenhaver Espino has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, VLP Copenhaver Espino 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. VLP Copenhaver Espino is providing the affected resident with notification of this incident, commencing on or about January 31, 2025. The notice will be in substantially the same form as the letter attached hereto. VLP Copenhaver Espino is also offering the affected resident a complimentary membership with a credit monitoring service. VLP Copenhaver Espino is advising the affected resident to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. VLP Copenhaver Espino is also advising the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected resident is being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission and the Maryland Attorney General Consumer Protection Division.

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

If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,

Spencer S. Pollock

[redacted]

[redacted]

VLP COPENHAVER ESPINO

000010102G0500 P

[redacted]

IMPORTANT INFORMATION, PLEASE REVIEW CAREFULLY

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to VLP Copenhaver Espino. VLP Copenhaver Espino is a Florida based law firm that received your information as part of legal proceedings with the federal government. We are writing with important information regarding a security incident that may have impacted some of your information. As such, we want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about September 18, 2024, VLP Copenhaver Espino detected unauthorized access to our network.

What We Are Doing.

Upon learning of this issue, we immediately secured the environment and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and document review, we discovered that between May 27, 2024, and September 18, 2024, certain impacted files containing personal information may have been accessed and/or acquired by an unauthorized individual.

What Information Was Involved?

The potentially impacted information includes your [redacted]

What You Can Do.

We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident. To protect you from potential misuse of your information, 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 twelve (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 the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services

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.

Please accept our apologies that this incident occurred. VLP Copenhaver Espino is committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. VLP Copenhaver Espino continually evaluates and modifies its practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

Respectfully,

VLP Copenhaver Espino
413 East Park Avenue
Tallahassee, Florida 32301

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary Credit Monitoring.

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. 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.

0001020280000

P

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. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. 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. Additional information is available at: https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/.

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 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 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	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, you will 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 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.

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. Obtain and Monitor Your 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. 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.

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 (Toll-free within North Carolina), 919-716-6000.

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.marylandattorneygeneral.gov, Telephone: 888-743-0023.