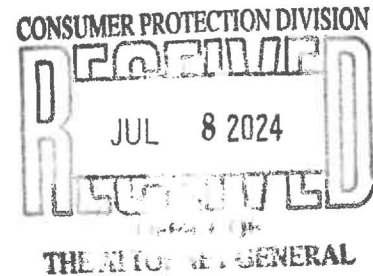


Dominic A. Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

July 1, 2024

VIA U.S. MAIL

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



Re: Heaven & Alvarez, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Heaven & Alvarez, LLC (“Heaven & Alvarez”). I am writing to provide notification of an incident at Heaven & Alvarez that may affect the security of personal information of approximately two (2) Maryland residents. By providing this notice, Heaven & Alvarez does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Heaven & Alvarez recently became aware of unauthorized access to its email tenant and accounting management system. Upon learning of this issue, Heaven & Alvarez launched an investigation and secured the tenant and management system. As part of the investigation, Heaven & Alvarez has been working very closely with third-party cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and thorough document review, Heaven & Alvarez discovered on June 6, 2024, that the unauthorized actor accessed one (1) employee email account and management program between February 1, 2024 and March 27, 2024. As a result, the threat actor potentially accessed certain files containing personal information pertaining to a limited number of Maryland residents. The information included residents’ full names and one or more of the following: Social Security number and bank/financial account number.

Nevertheless, Heaven & Alvarez 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. Heaven & Alvarez is providing the affected residents with written notification of this incident commencing on or about July 1, 2024, in substantially the same form as the letter attached hereto. Heaven & Alvarez is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents whose Social Security numbers were impacted are being offered complimentary credit monitoring for one year. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At Heaven & Alvarez, protecting the privacy of personal information is a top priority. Heaven & Alvarez is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Heaven & Alvarez 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 248-220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in blue ink, appearing to read 'DPaluzzi', is centered below the 'Sincerely,' text.

Dominic A. Paluzzi

Encl.

HEAVEN
&
ALVAREZ
CERTIFIED PUBLIC ACCOUNTANTS

[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Heaven & Alvarez, LLC ("Heaven & Alvarez"). We are writing with important information regarding a recent data security incident that potentially involved some of your personal information. As such, we want 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 information.

What Happened?

On March 27, 2024, Heaven & Alvarez detected unauthorized access to our network environment.

What We Are Doing

Upon learning of this issue, we secured the network and launched an investigation. As part of the investigation, we have been working very closely with third-party cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and thorough manual review, we determined on June 6, 2024, that certain files containing your personal information may have been accessed and/or acquired by an unauthorized individual(s).

What Information Was Involved?

The potentially impacted information may include your full name and [REDACTED]

What You Can Do

Out of an abundance of caution, we want to make you aware of the incident. To protect you from the potential misuse of your information, we are offering a complimentary [REDACTED] month membership with Identity Defense Complete credit and identity monitoring. For more information on identity theft prevention and the credit-monitoring product being offered to you, including instructions on how to activate your complimentary [REDACTED] month 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/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 for fraudulent or irregular activity on a regular basis. For more information and instructions on how to activate your complimentary Identity Defense membership, please review the "Other Important Information" section.

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 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, [REDACTED].

Sincerely,

Heaven & Alvarez

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring.



Identity Defense

Enter your Activation Code: [REDACTED]

Enrollment Deadline: [REDACTED]

Service Term: [REDACTED]

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

To enroll in Identity Defense, visit [REDACTED]

1. Enter your unique Activation Code [REDACTED]
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is [REDACTED]. After [REDACTED], the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by [REDACTED], you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at [REDACTED].

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 one-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) 685-1111

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

3. Consider 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 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(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 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. 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. 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.

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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

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.