

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

April 19, 2024

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

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

Re: Avalon Trust – Incident Notification

Dear Mr. Brown

McDonald Hopkins PLC represents Avalon Trust (located at 125 Lincoln Ave # 301, NM 87501). I am writing to provide notification of an incident at Avalon Trust that may affect the security of personal information of one (1) Maryland resident. By providing this notice, Avalon Trust does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On April 24, 2023, Avalon Trust identified an outgoing spam email campaign that appeared to be from one of its employee email accounts. After discovering the incident, Avalon Trust engaged our firm and third-party independent cybersecurity experts to conduct a thorough investigation of the nature and scope of the incident. Avalon Trust recently concluded its investigation, which revealed that an unauthorized actor gained access to two (2) of its employees' email accounts, and as a result, potentially viewed personal information. On March 13, 2024, after an extensive forensic investigation and review, Avalon Trust discovered that certain personal information was included within the data that may have been viewed by the unauthorized actor. The personal information potentially viewed included name and tax identification number. We have no evidence indicating that information has been used for identity theft or financial fraud as a result of the incident.

Avalon Trust wanted to inform you (and the affected resident) of the incident and explain the steps that it is taking to help safeguard the affected resident against identity fraud. Avalon Trust is providing the affected resident with written notification of this incident commencing on or about April 19, 2024 in substantially the same form as the letter attached hereto. Avalon Trust 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

April 19, 2024

Page 2

with the contact information for the Maryland Attorney General's office, the consumer reporting agencies and the Federal Trade Commission.

At Avalon Trust, protecting the privacy of personal information is a top priority. Avalon Trust is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Avalon Trust 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) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



James J. Giszczak

Encl.

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

April 19, 2024

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Avalon Trust. We are writing to let you know about a data security incident that involved some of your personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened?

On April 24, 2023, we discovered an outgoing spam email campaign that appeared to be from one of our employee email accounts. When we discovered the suspicious activity, our technology team acted quickly to secure our systems. We also engaged third-party cybersecurity experts to conduct an investigation to determine the full nature and scope of the event.

At the conclusion of the initial investigation, we determined that an unauthorized actor gained access to two (2) of our employees' email accounts, and as a result, potentially viewed your personal information. With the results of the investigation, we began a comprehensive review of the affected employees' email accounts.

Our comprehensive investigation and review recently concluded on March 13, 2024 and determined that your information was included within the data that may have been viewed by the unauthorized actor. Based on our investigation, and the nature of the unauthorized account activity, we believe this was solely an attempt to cause an invoice payment to be misdirected to a fraudulent account (which, to the best of our knowledge, was not successful), and **we have no evidence that your information has been used for identity theft or financial fraud**. However, we wanted to notify you of the incident out of an abundance of caution and provide you information on how to best protect your identity.

What Information Was Involved.

The information involved in the incident included your first and last name and your [REDACTED]
[REDACTED] ***To reiterate, we have no evidence indicating that your information has been used for identity theft or financial fraud as a result of the incident.***

What We Are Doing.

The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic and legal experts to assist in the investigation. Additionally, while we have safeguards in place to protect data in our care, we continue to review and further enhance these protections as part of our ongoing commitment to data security.

What You Can Do.

As stated above, while we have no evidence indicating that your information has been used for identity theft or fraud, this letter provides 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. If your bank account 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. 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. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it.

If you have any further questions regarding this incident, please contact [REDACTED] at [REDACTED] or [REDACTED].

Sincerely,

Avalon Trust
125 Lincoln Ave # 301
Santa Fe, NM 87501

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

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 30348-5788
<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 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.

5. Protecting Your Medical Information.

The following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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.

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.