

Spencer S. Pollock
Direct Dial: (410) 917 5189
E-mail: spollock@mcdonalddhopkins.com

January 12, 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: Etkin Management LLC – Incident Notification

Dear Mr. Brown:

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

On March 31, 2023, Etkin detected unauthorized access within their network environment. Upon detection of the incident, Etkin immediately commenced a prompt and thorough investigation with external cybersecurity professionals experienced in handling these types of incidents. As part of the investigation, Etkin worked to identify what personal information, if any, might have been present in the accessed and acquired systems.

After a thorough forensic investigation and extensive manual review, Etkin discovered on December 13, 2023, that an unauthorized party potentially accessed and acquired files from the network acquired in connection with this incident. This information included full name and Social Security Number.

Etkin is not aware of any reports of identity theft or fraud as a direct result of this incident. However, out of an abundance of caution, Etkin wanted to inform your Office (and the affected residents) of the incident. Affected residents will be notified of the incident starting on January 12, 2024. Notified individuals will be provided with best practices to protect their information. Etkin will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Etkin 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.

January 12, 2024

Page 2

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

Should you have any questions regarding this notification, please contact me at (410) 917-5189 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Spencer S. Pollock

Encl.

Etkin Management LLC
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08314



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

January 12, 2024

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Etkin Management LLC ("Etkin"). We are writing with important information regarding a recent security incident that involved some of your personal information. We want to provide you with information about the incident, explain the services being made available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On March 31, 2023, Etkin detected unauthorized access within our network environment.

What We Are Doing

Upon learning of this issue, Etkin contained the threat and immediately commenced a prompt and thorough investigation with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and comprehensive manual document review, Etkin discovered on December 13, 2023, that some of your personal information may have been accessed and acquired in connection with this incident.

What Information Was Involved

The potentially accessed and acquired information included your full name and [REDACTED]

What You Can Do

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We are also providing complimentary Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twenty-four 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 about Cyberscout and instructions on how to enroll, please see the Other Important Information section 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. To the extent that it is helpful, we have included information about protecting you against medical identity theft.

For More Information

Please accept our apologies that this incident occurred. Etkin is 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 help protect against potential misuse of your information. The response line is available Monday through Friday 8:00 am – 8:00 pm EST (excluding major U.S. holidays).

Sincerely,

Etkin Management LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/etkin> 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.

2. 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

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.

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.

6. 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.

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.