



A business advisory and advocacy law firm®

600 Superior Avenue East
Suite 2100
Cleveland, OH 44114

P 216.348.5400
F 216.348.5474

Beth Gillin
Direct Dial: 216.348.5457
E-mail: bgillin@mcdonaldhopkins.com

August 29, 2024

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

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

Re: Goodwin House Incorporated – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Goodwin House Incorporated (“Goodwin”). I am writing to provide notification of an incident at Goodwin that may affect the security of personal information of approximately one hundred and seventy (170) Maryland residents.¹ By providing this notice, Goodwin does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Goodwin Living discovered that one employee account was accessed by an unauthorized actor between October 2, 2023 and October 18, 2023. Upon learning of this issue, Goodwin Living immediately took steps to secure its network environment and commenced a prompt and thorough investigation. As part of its investigation, Goodwin Living has been working closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, Goodwin Living determined on July 30, 2024 that the impacted email account contained personal and protected health information included the impacted residents’ full name and Social Security number, medical information, and health insurance information.

To date, Goodwin is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Goodwin 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. Goodwin is providing the affected residents with written notification of this incident commencing on or about August 29, 2024 in substantially the same form as the letter attached hereto. Goodwin 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 with impacted Social Security numbers 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 Federal Trade Commission, and the Maryland Attorney General Consumer Protection Division.

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

¹ There were 170 individuals with a Maryland address notified under Maryland state law; however an additional 212 individuals with a Maryland address were notified under the Health Insurance Portability and Accountability Act Breach Notification Rule, 45 C.F.R. §§ 164.400-414 (“HIPAA” or “Final Rule”). The 212 individuals notified under HIPAA had impacted data elements that are defined as PII under Maryland law.

Should you have any questions regarding this notification, please contact me at 216.348.5474 or bgillin@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in black ink that reads "Beth Gillin". The script is cursive and fluid, with the first name "Beth" and last name "Gillin" clearly distinguishable.

Beth Gillin

Encl.

Goodwin House Incorporated
c/o Cyberscout
PO Box 179
Manchester, NH 03105



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to Goodwin House Incorporated (doing business as “ Goodwin Living”). We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved some of your personal and/or protected health information. As such, 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 information.

What Happened?

Goodwin Living discovered that one employee email account was accessed by an unauthorized actor between October 2, 2023 and October 18, 2023.

What We Are Doing.

Upon learning of this issue, Goodwin Living immediately took steps to secure our network 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. Following this investigation and manual document review, we determined on July 30, 2024 that the impacted email account that was accessed between October 2, 2023 and October 18, 2023 contained a limited amount of personal and protected health information that may have been accessed or acquired by the unauthorized party.

What Information Was Involved?

The impacted email account contained some of your personal and/or protected health information, including your [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. To protect you and your information, we are providing you with [REDACTED] months of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. These services provide you with alerts for [REDACTED] 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.

000010103G0500

P

The credit monitoring services are completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and the credit monitoring services, including instructions on how to activate your complimentary [REDACTED] membership, please see the additional information provided in this letter. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

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, explanation of benefits, and credit reports for fraudulent or irregular activity on a regular basis.

For More 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 to 8:00 pm Eastern time, (excluding major U.S. holidays).

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 information.

Sincerely,

Goodwin Living
4800 Fillmore Avenue,
Alexandria, VA 22311

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring

In response to the incident, 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 [REDACTED] 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, a TransUnion 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. 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.

Whether or not you choose to use the complimentary [REDACTED] month credit monitoring services, we recommend that you place a 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
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800



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 such as copy of a government issued identification. 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. 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 the 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 disclosure (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 care provider for any items you do not recognize.

6. 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.

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.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.



00001030300000

P

