

June 17, 2022

Rachel H Cobble
205.709.8991 (direct)
423.653.9044 (mobile)
Rachel.Cobble@wilsonelser.com

Via electronic-mail: Idtheft@oag.state.md.us

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

Re:	Our Client	:	MKRDY Ogunquit, LLC
	Matter	:	3/25/22 Data Security Incident
	Wilson Elser File #	:	16516.1815

Dear Attorney General Frosch:

We represent MKRDY Ogunquit, LLC (hereinafter “MKRDY Ogunquit”), located in Dallas, Texas with respect to a data security incident described in more detail below. MKRDY Ogunquit takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, and the steps that the MKRDY Ogunquit is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On March 25, 2022, MKRDY Ogunquit was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate MKRDY Ogunquit’s computer systems. This incident may have resulted in the exposure of personal information that was located on MKRDY Ogunquit’s systems, including full name, address and social security number. This information was maintained consistent with an employer-employee relationship, including standard administrative and payroll functions.

MKRDY Ogunquit is not aware of any evidence that information has been misused and has not received any reports of related identity theft since the date of the incident.

2. Number of Maryland Residents Affected

A total of one (1) resident of Maryland was potentially affected by this security incident. A notification letter to this individual was mailed on June 3, 2022 by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, MKRDY Ogunquit moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. MKRDY Ogunquit has enhanced its technical safeguards relating to the security of its systems and servers to protect against a future incident.

4. Contact Information

MKRDY Ogunquit remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Rachel.Cobble@WilsonElser.com or 205.709.8991.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Rachel H. Cobble, Esq.

Copy: Robert Walker, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

MKRDY Ogunquit LLC
c/o of Cyberscout, a Transunion Company
P.O. Box 3923
Syracuse, NY 13220

June 3, 2022

Notice of Data Breach

Cliff House Maine, operated under the management entity of MKRDY Ogunquit LLC, in Cape Neddick Maine is writing to inform you of an incident that may have exposed your sensitive personal information. We take the privacy of personal information seriously. For these reasons, we want to provide you with information related to the incident, as well as our plan for notifying individuals.

What happened?

Cliff House Maine detected and stopped a network security incident on March 25, 2022. An unauthorized third-party infiltrated our network. We immediately engaged specialized third-party forensic and technical resources to respond to the incident. Cliff House Maine has secured and remediated its network and the data that we maintain.

What information was involved?

Although we have no evidence that your information was specifically misused, the results of the forensic investigation have revealed it is possible your full name, address, and social security number may have been exposed to an unauthorized party from stored data in January 2015 through March 2019.

What are we doing?

Once our environment was secure, we initiated a comprehensive investigation into the extent of the unauthorized activity. As of the writing, we have not received any reports of related identity theft since the date of the incident.

We have made immediate enhancements to our systems, security and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation. We have also reported the matter to the F.B.I.

To help relieve concerns and restore confidence following this incident, we are offering identity theft protection services through Cyberscout, a company specializing in fraud assistance and remediation services. Services include identity protection and resolution services, \$1,000,000 identity theft insurance policy, and access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve 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. In addition, we are providing you with

* Services marked with an "*" require 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.

proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

How do I enroll for the free services?

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: **131tctn0ljde** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What can I do on my own to address this situation?

If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Cliff House Maine

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Cyberscout at 1-800-405-6108 Monday through Friday, 8:00 am to 8:00 pm Eastern time. While representatives should be able to provide thorough assistance and answer most of your questions, you may still

* Services marked with an "*" require 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.

feel the need to speak with Cliff House Maine regarding this incident. If so, please call Keith Burke at 207-361-6222 from 8:30 am to 4:30 pm Eastern Time, Monday through Friday.

We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at listed above.

* Services marked with an “*” require 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.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

* Services marked with an “*” require 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.