

Paul F. Schmeltzer
T (213) 417-5163
F +121348811
Email:pschmeltzer@ClarkHill.com

Clark Hill LLP
1055 West Seventh Street, Suite 2400
Los Angeles, CA 90017
T (213) 891-9100
F +12134881178

January 9, 2022

Via email: Idtheft@oag.state.md.us

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

Dear Mr. Frosh:

We represent Sunset Harbour Yacht Club (“Sunset Harbour”) with respect to a data security incident involving the unauthorized access of limited personally identifiable information (“PII”) described in more detail below. Sunset Harbour is committed to answering any questions you may have about the data security incident its response and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On March 26, 2021, Sunset Harbour identified suspicious activity on its U.S. based email network. Sunset Harbour engaged an independent computer forensic firm to assist in responding to and investigating this incident and a law firm specializing in these matters to oversee this investigation. The investigators determined that someone had gained unauthorized access to one Sunset Harbour email account on March 26, 2021. Though there was no evidence of any malicious activity associated with this access, Sunset Harbour investigated the account to determine what information was found in those accounts, whether it constituted personal information, or other confidential information, and to whom that information belonged. This process took a considerable amount of time and only concluded on December 10, 2021.

2. Number of residents affected.

Three (3) Maryland residents may have been affected and were notified of the incident. A notification letter is being sent to the potentially affected individual on January 10, 2022 (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

Sunset Harbour took steps to address this incident and prevent similar incidents in the future. All passwords have been reset throughout the email system, encrypted email was set up for all users to allow for end-to-end email encryption to protect email transmissions, and Sunset Harbour replaced Symantec with their new Cloud Bitdefender Gravity Zone and ran security scans on all systems/server.

Additionally, Sunset Harbour has also arranged for affected individuals to receive single bureau credit monitoring, single bureau credit report, and single bureau credit score, and cyber monitoring services at no cost for twenty-four months from the date of enrollment. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

4. Contact information.

Sunset Harbour takes the security of information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at pschmeltzer@clarkhill.com or (213) 417-5163.

Sincerely,

CLARK HILL



Paul F. Schmeltzer
Attorney
cc: Jason Schwent

Enclosure

Sunset Harbour Yacht Club
P.O. Box 3923
Syracuse, NY 13220

January 10, 2022

Notice of Data Breach

Dear :

Sunset Harbour Yacht Club (“Sunset Harbour”) values its relationship with you and understands the importance of protecting your personal information. We are writing to inform you of a data security incident that occurred.

While we have no evidence that any of your personal information was accessed, acquired or misused, out of an abundance of caution, we are providing you notice and outlining proactive steps to protect your personal information. This letter also describes credit protection services Sunset Harbour is providing to you free of charge, and resources being made available to help you.

What happened?

On March 26, 2021, Sunset Harbour identified suspicious activity on its U.S. based email network. Sunset Harbour engaged an independent computer forensic firm to assist in responding to and investigating this incident and a law firm specializing in these matters to oversee this investigation.. The investigators determined that someone had gained unauthorized access to one Sunset Harbour email account on March 26, 2021. Though there was no evidence of any malicious activity associated with this access, Sunset Harbour investigated the account to determine if any personal information was located in the email account.

On December 10, 2021, it was determined that some personal information was in the sole affected email account. While there is no evidence of unauthorized access or acquisition or misuse of your personal information, out of an abundance of caution, Sunset Harbour is providing you with notice of this incident.

What Information Was Involved?

Based on the investigation, the information contained in the sole impacted account could have included a combination of the following: Account Number, Financial Institution Name.

What we are doing:

We want to assure you that Sunset Harbour has taken steps to prevent this event from happening in the future. Following the incident, all passwords have been reset throughout the email system, encrypted email was set up for all users to allow for end-to-end email encryption to protect email transmissions,

and we replaced Symantec with our new Cloud Bitdefender Gravity Zone and ran security scans on all systems/server.

Additionally, Sunset Harbour has also arranged for you to receive Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring* services at no cost to you. These services provide you with alerts for twenty-four months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. 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 company specializing in fraud assistance and remediation services.

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.

What you can do:

While we believe it is unlikely that any of your information will be misused, it is always a good idea to review your credit reports and financial statements for any suspicious activity. You can also visit <https://www.consumer.ftc.gov/topics/privacy-identity-online-security> for more information on how to protect yourself online.

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: **ky1u4pz95xp6** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

For more information

We sincerely regret that this incident occurred. Sunset Harbour remains committed to protecting the privacy and security of personal information of its members. If you have questions, please contact me at 305-398-6800 or dprieto@sunsetharbouryc.com.

Sincerely,

Daniel Prieto, CMO
General Manager
Sunset Harbour Yacht Club

* 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.

Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://www.myidmanager.com> and follow the instructions for enrollment using your Enrollment Code referenced above.
- 2. Activate the credit monitoring** provided as part of your services with Cyberscout. The monitoring included must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, Cyberscout will be able to provide guidance.
- 3. Telephone.** Contact Cyberscout at 1-800-405-6108 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in Cyberscout credit monitoring, notify them immediately by calling 1-800-405-6108 from 8:00 am to 8:00 pm Eastern, Monday through Friday.

A representative will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be able to work with a representative who will assist you with resolving any fraudulent activity.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

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; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There was 1 Rhode Island resident impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.