

July 19, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email:

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving Atlantic Coast Athletic Clubs

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Atlantic Coast Athletic Clubs (“ACAC”), an athletic club, with respect to a recent cybersecurity incident that was first discovered by ACAC on June 20, 2022 (hereinafter, the “Incident”). ACAC takes the security and privacy of the information in its control very 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 Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that ACAC has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted businesses.

1. Nature of the Incident

On June 20, 2022, ACAC discovered that an unauthorized individual potentially accessed files containing ACAC employee data. ACAC immediately began a thorough review of the potentially accessed files to identify the employees whose sensitive information may have been compromised.

The forensic investigation is currently ongoing and ACAC will proceed to notify additional individuals once the investigation has completed.

2. Nature of Personal Information

Although ACA is unaware of any fraudulent misuse of information, it is possible that individuals’ full name and social security number may have been exposed as a result of this unauthorized activity.

As of this writing, ACAC has not received any reports of related identity theft since the date of the incident (June 20, 2022 to present).

3. Number of Maryland residents affected.

A total of eight hundred and forty-six (846) Maryland residents have been potentially affected by this incident. Notification letter to individuals was mailed July 19, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

4. Steps taken in response to the Incident.

ACAC is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, ACAC moved quickly to investigate and respond to the Incident, assessed the security of its systems, and will be notifying the potentially affected individuals. Specifically, ACAC engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. In response to the Incident, ACAC has started an internal investigation to ascertain how this Incident occurred, changed passwords on all accounts, implemented Huntress and Sentinel One, moved accounting software to the cloud, created a new email server, created a new domain controller, and a new file share.

Although ACAC is not aware of any actual or attempted misuse of the affected personal information, ACAC will be offering twelve (12) months of complimentary credit monitoring and identity theft restoration services to individuals to help protect their identity. Additionally, ACAC provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

5. Contact information

ACAC 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 Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A



P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-909-4420

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

July 19, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

Atlantic Coast Athletic Clubs ("ACAC") is writing to inform you of a recent cybersecurity incident ("Incident") that may have involved your personal information. At this time, we have no evidence that your information has been misused. However, out of an abundance of caution we are alerting you that the Incident occurred. ACAC takes the privacy of its employees' information very seriously and sincerely apologizes for any inconvenience this Incident may cause. This letter contains details about the Incident, steps we have taken in response to mitigate any risk, and services we are making available to protect your information.

What Happened?

On June 20, 2022, ACAC discovered that an unauthorized individual potentially accessed files containing ACAC employee data. After learning about this Incident, ACAC promptly engaged a third party cybersecurity firm to conduct a forensics investigation to analyze the nature and scope of the Incident, and to determine whether any employee information may have been exposed as a result of the Incident. At this time, the investigation is still ongoing.

What Information Was Involved?

Our investigation to date indicates that certain files containing employee information may have been subject to unauthorized access. These files may include one or more of the following types of employee data: Name and Social security number. At this time, while ACAC cannot confirm with certainty that your information has been accessed, we are nonetheless notifying you so that you can take steps to protect yourself.

What We Are Doing

ACAC takes the privacy and security of our employees' information very seriously, and has taken steps to prevent a similar event from occurring in the future. In response to the Incident, ACAC has started an internal investigation to ascertain how this Incident occurred, changed passwords on all accounts, implemented Huntress and Sentinel One, moved accounting software to the cloud, created a new email server, created a new domain controller, and a new file share.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft restoration. With this protection, IDX will help individuals resolve issues if they believe their identity has been compromised.

What You Can Do

Although ACAC is not aware of any instances of misuse of any information, we recommend that our employees take advantage of the complimentary services that are being offered. Instructions on how to enroll in these services are included in the materials enclosed with this letter. We also encourage our employees to remain vigilant and review the enclosed addendum titled “*Additional Important Information*” outlining additional steps you can take to protect your information.

We encourage employees to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that contacting any financial institutions and all major credit bureaus to inform them of a potential breach and then take whatever steps are recommended, including the possible placement of a fraud alert on credit files. Please review the enclosed *Additional Important Information*, to learn more about how to protect against the possibility of information misuse.

We also encourage employees to contact IDX with any questions and to enroll in free identity protection services by going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. Please note, the deadline to enroll is October 19, 2022.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who 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 assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

Other Important Information

You will need to reference the enrollment code at the top of this letter enrolling online, so please do not discard this letter.

ACAC recognizes that you may have questions not addressed in this letter. If you have additional questions please do not call ACAC Human Resources. Instead, please call 1-833-909-4420 during the 7 am to 7 pm Mountain Time, Monday through Friday (excluding U.S. national holidays).

Sincerely,



Chris Craytor, CEO

Additional Important 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.

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

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Identity Protection PIN: You can get a six-digit Identity Protection PIN to prevent someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. An IP PIN is used by the IRS to verify your identity when filing your electronic or paper tax return. To receive an IP Pin, you must register to validate your identity at IRS.gov. Use the Get an IP PIN tool available between mid-January through mid-November to receive your IP PIN.

<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>

Security Freeze: You 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:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 at 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 residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

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

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov