

February 19, 2025

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

**Via Email:**

Attorney General Anthony G. Brown  
**Office of the Attorney General**  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
[Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)

**Re: Cybersecurity Incident Involving Waynesborough Country Club Of Chester County Inc.**

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Waynesborough Country Club Of Chester County Inc. (“WCC”), a country club in 440 Darby Paoli Road, Paoli, PA 19301, with respect to a recent data privacy incident that was first discovered by WCC on or around December 19, 2024 (hereinafter, the “Incident”). WCC 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 WCC has taken in response to the Incident. We have also enclosed hereto a sample of the notification that will be made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

**1. Nature of the Incident**

On or about December 19, 2024, WCC detected unusual activity within its computer systems. Upon discovery of this incident, WCC promptly engaged a specialized third-party cybersecurity firm and IT vendor to assist with securing the systems in question, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that certain data contained in the computer systems was accessible by an unauthorized actor.

Based on the findings of the forensic investigation, WCC conducted a comprehensive review of the contents of the systems to identify specific individuals and types of information that may have been impacted. Since that time, WCC has been thoroughly reviewing its files to obtain the last known addresses for the affected individuals and to remove duplicates on the list. On February 12, 2025, WCC finalized the list of individuals to notify.

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

As of this writing, WCC has not received any reports of related identity theft since the date of the incident (December 19, 2024 to present).

**2. Number of Maryland residents affected.**

A total of one [1] Maryland resident(s) may have been potentially affected by this incident. Notification letters to these individuals will be mailed on or around February 21, 2025, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

**3. Steps taken in response to the Incident.**

WCC 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, WCC moved quickly to investigate, respond, and confirm the security of its systems. Specifically, WCC engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, WCC changed all user credentials, trained or retrained workforce members, enhanced the security measures (including MFA), and took steps and will continue to take steps to mitigate the risk of future harm. Lastly, WCC informed Wilson Elser and began identifying the potentially affected individuals in preparation for notice.

Although WCC is not aware of any actual or attempted misuse of the affected personal information, WCC is offering 12 months of complimentary credit monitoring and identity theft restoration services through Haystack to all individuals to help protect their identity. Additionally, WCC 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.

**4. Contact information**

WCC 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](mailto:Anjali.Das@WilsonElser.com) or 312-821-6164.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



Anjali C. Das

## **EXHIBIT A**



Waynesborough Country Club  
c/o Return Processing Center  
P.O. Box 3826  
Suwanee, GA 30024



February 21, 2025

**Re: Data Security Incident**

Dear 

Waynesborough Country Club Of Chester County Inc. (“WCC”) is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive personal information. We are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

**What Happened?** On or about December 19, 2024, WCC detected unusual activity within its computer systems. Upon discovery of this incident, WCC promptly engaged a specialized third-party cybersecurity firm and IT vendor to assist with securing the systems in question, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that certain data contained in the computer systems was accessible by an unauthorized actor.

Based on the findings of the forensic investigation, WCC conducted a comprehensive review of the contents of the systems to identify specific individuals and types of information that may have been impacted. Since that time, WCC has been thoroughly reviewing its files to obtain the last known addresses for the affected individuals and to remove duplicates on the list. On February 12, 2025, WCC finalized the list of individuals to notify.

**What Information Was Involved?** Based on the investigation, the following information related to you may have been subject to unauthorized access: name; Social Security Number.

**What We Are Doing.** WCC takes the security of its employee’s and member’s information very seriously, and has taken steps to prevent a similar event from occurring in the future. Since the discovery of the incident, WCC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, WCC engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, WCC changed all user credentials, trained or retrained workforce members, enhanced the security measures (including MFA), and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the incident, WCC is 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 12 months from the date of enrollment when changes occur to your credit file. A 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 HaystackID, specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Resources To Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

**How do I enroll for the free services?** To enroll in Credit Monitoring services at no charge, please log on to [www.privacysolutions.com](http://www.privacysolutions.com) 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.

We encourage you to take full advantage of the services offered.

**For More Information.** If you have any questions or concerns not addressed in this letter, please call 888-244-3060 (toll free) Monday through Friday, during the hours of 9 a.m. and 9 p.m. Eastern Standard Time, Monday through Friday, excluding U.S. national holidays.

WCC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

**WAYNESBOROUGH COUNTRY CLUB OF CHESTER COUNTY INC.**

## **ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION**

**Monitor Your Accounts.** We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

**Credit Freeze.** You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

**Fraud Alert.** You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

**Federal Trade Commission.** For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

**Contact Information.** Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

| <b>Credit Reporting Agency</b> | <b>Access Your Credit Report</b>                                                                                      | <b>Add a Fraud Alert</b>                                                                                                                                              | <b>Add a Security Freeze</b>                                                                                                                                                          |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Experian</b>                | P.O. Box 2002, Allen, TX 75013-9701<br><br>1-866-200-6020<br><a href="http://www.experian.com">www.experian.com</a>   | P.O. Box 9554, Allen, TX 75013-9554<br><br>1-888-397-3742<br><a href="https://www.experian.com/fraud/center.html">https://www.experian.com/fraud/center.html</a>      | P.O. Box 9554, Allen, TX 75013-9554<br><br>1-888-397-3742<br><a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>                             |
| <b>Equifax</b>                 | P.O. Box 740241, Atlanta, GA 30374-0241<br><br>1-866-349-5191<br><a href="http://www.equifax.com">www.equifax.com</a> | P.O. Box 105069, Atlanta, GA 30348-5069<br><br>1-800-525-6285<br><a href="http://www.equifax.com/personal/credit-report-">www.equifax.com/personal/credit-report-</a> | P.O. Box 105788, Atlanta, GA 30348-5788<br><br>1-888-298-0045<br><a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a> |

|                   |                                                                                      |                                                                                              |                                                                                           |
|-------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|                   |                                                                                      | services/credit-fraud-alerts                                                                 |                                                                                           |
| <b>TransUnion</b> | P.O. Box 1000,<br>Chester, PA 19016-1000<br><br>1-800-888-4213<br>www.transunion.com | P.O. Box 2000, Chester,<br>PA 19016<br><br>1-800-680-7289<br>www.transunion.com/fraud-alerts | P.O. Box 160, Woodlyn, PA 19094<br><br>1-800-916-8800<br>www.transunion.com/credit-freeze |

**Iowa and Oregon residents** are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

**Massachusetts residents** are advised of their right to obtain a police report in connection with this incident.

**District of Columbia residents** are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6<sup>th</sup> St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at [consumer.protection@dc.gov](mailto:consumer.protection@dc.gov).

**Maryland residents** can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

**New York residents** are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/) or <https://www.identitytheft.gov/#/>.

**North Carolina residents** are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting [www.ncdoj.gov](http://www.ncdoj.gov), or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

**Rhode Island residents** are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.