



March 24, 2025

Daniel Parziale

504.702.1712 (direct)

[Daniel.Parziale@WilsonElser.com](mailto:Daniel.Parziale@WilsonElser.com)

**Via Electronic Mail:** [Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)

**Office of the Attorney General**

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

**Re: Cybersecurity Event Involving Westwood Country Club.**

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Westwood Country Club (“Westwood”), located at 11801 Conway Road, St. Louis MO, 63131, with respect to a recent cybersecurity event that was first discovered by Westwood on October 17, 2025 (hereinafter, the “Event”). Westwood takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar Event from occurring in the future.

This letter will serve as notice of the nature of the Event, what information may have been compromised, the number of Maryland residents being notified, and the steps that Westwood has taken in response to the Event. We have also included with this letter a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services. By providing this notice, the Westwood does not waive any rights or defenses regarding the applicability of the Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

**1. Nature of the Event**

On October 17, 2024, Westwood detected suspicious activity in its network environment. Upon discovery of this incident, Westwood promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Westwood learned that an unauthorized actor accessed and copied certain files within the network environment.

Upon learning this, and with the help of a data mining vendor, Westwood began a time-consuming and detailed reconstruction and review of the data stored on their servers at the time of this incident to understand whose information may be affected. On March 14, 2025, Westwood identified persons whose sensitive data may have been included within the impacted

data. The following types of information may have been impacted: Name, and Social Security number.

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

A total of 6 Maryland resident(s) may have been potentially affected by this event. Notification letters to these individuals were mailed on March 24, 2025, via 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 Event.**

Westwood remains committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar Event from occurring in the future in addition to its already robust security controls. Upon discovery of the Event, Westwood moved quickly to investigate and respond to the Event, assessed the security of its systems, and notified the potentially impacted individuals in an abundance of caution. Specifically, Westwood engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Event. Westwood informed our law firm and began identifying the potentially impacted individuals in preparation for notice as soon as possible under the circumstances. Although Westwood is not aware of any actual or attempted misuse of the personal information at issue, Westwood offered 24 months of complimentary credit monitoring and identity theft restoration services.

**4. Contact information**

Westwood 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 Daniel.Parziale@WilsonElser.com or 504.702.1712.

Regards,

A handwritten signature in cursive script that reads "Daniel Parziale". The signature is written in dark ink and is positioned above a horizontal line.

**Daniel Parziale**

Wilson Elser Moskowitz Edelman & Dicker LLP

# **Exhibit A**

Westwood Country Club  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998

Via First-Class Mail



March 24, 2025

Dear [REDACTED]:

Westwood Country Club (“Westwood” or “we”) writes to inform you of a recent event that may impact some of your personal information. Westwood takes this event seriously and the privacy, security, and confidentiality of information in our care is among our highest priorities. While Westwood is not aware of any actual or attempted misuse of your information to perpetrate financial fraud, out of an abundance of caution, we are providing you with an overview of the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

### **What Happened?**

On October 17, 2024, Westwood detected suspicious activity in its network environment. Upon discovery of this incident, Westwood promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Westwood learned that an unauthorized actor accessed and copied certain files within the network environment.

Upon learning this, and with the help of a data mining vendor, Westwood began a time-consuming and detailed reconstruction and review of the data stored on their servers at the time of this incident to understand whose information may be affected. On March 14, 2025, Westwood identified persons whose sensitive data may have been included within the impacted data.

### **What Information Was Involved?**

Westwood determined that the information related to you that may have been copied without authorization as a result of the event, your name and Social Security number, Driver's license number, financial account information, health insurance information, and medical information.

### **What We Are Doing?**

The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved promptly to investigate and respond to the event and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. As an added precaution, 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 twenty-four (24) 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.

000010102G0500

P

**What You Can Do.**

You can learn more about how to help protect yourself against potential information misuse in the enclosed *Steps You Can Take To Help Protect Personal Information*. There, you will find instructions on how to activate in the complimentary credit monitoring. We also encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credits reports for suspicious activity, and to report any suspicious activity promptly to your bank, credit card company, or other applicable institution.

**For More Information.**

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-998-7238, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,

**Westwood Country Club**

## Steps You Can Take To Help Protect Personal Information

### **Activate in Monitoring Services**

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. Please note that the code is case-sensitive and will need to be entered as it appears.

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. Once enrolled you will have twenty-four (24) months of monitoring services. At the end of twenty-four (24) months, the services will be deactivated. 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.

### **Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.



00001020280000

P

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

| <b>Equifax</b>                                                                                                                  | <b>Experian</b>                                                             | <b>TransUnion</b>                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a> | <a href="https://www.experian.com/help/">https://www.experian.com/help/</a> | <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045                                                                                                                  | 1-888-397-3742                                                              | 1-800-916-8800                                                                              |
| Equifax Fraud Alert, P.O. Box 105069<br>Atlanta, GA 30348-5069                                                                  | Experian Fraud Alert, P.O. Box 9554,<br>Allen, TX 75013                     | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016                                    |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788                                                                   | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013                      | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094                                   |

### **Additional Information**

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Westwood Country Club is located at 11801 Conway Rd, St. Louis, MO 63131 and can be reached 314.432.2315 ext. 242.

*For New Mexico residents*, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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](http://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 New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).