



Jason M. Schwent  
T (312)985-5564  
F (312)985-5939  
Email:jschwent@clarkhill.com

Clark Hill  
130 E. Randolph Street, Suite 3900  
Chicago, Illinois 60601  
T (312) 985-5900  
F (312) 985-5999

October 18, 2024

**VIA EMAIL**

Office of the Attorney General  
Identity Theft Unit  
200 St. Paul Place  
Baltimore, MD 21202  
[IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

Dear Attorney General Brown,

We represent Woodloch Pines and the Lodge at Woodloch (“collectively Woodloch Properties”) with respect to a data security incident involving personal information as described below. Woodloch Properties is a resort and spa located in Hawley, Pennsylvania. Woodloch Properties takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

**1. Nature of security incident**

On or around May 4, 2024, Woodloch Properties identified suspicious activity within its network. Woodloch Properties immediately implemented its incident response protocols, took steps to secure the environment, and engaged independent computer forensic experts to assist with an investigation. The investigation found that there was unauthorized access to systems for a limited period of time. The investigation also determined that files within the systems were accessed during the period of unauthorized access. Woodloch Properties reviewed the contents of the files accessed to identify the types of personal information found within those files and the individuals who were associated with that information so that notice could be provided. This review was completed on October 3, 2024 and it was determined that personal information was potentially impacted.

Impacted information includes names with some combination of the following: addresses, dates of birth, Social Security numbers, driver’s license or state ID numbers, financial account information, passport numbers, payment card information, taxpayer ID numbers, medical information, and health insurance policy information.

**2. Number of Maryland residents affected**

Sixteen (16) Maryland residents were notified of the incident. Notification letters were sent to potentially affected individuals on October 18, 2024. A copy of the template notification letter is attached as Exhibit A.

### **3. Steps taken in response to the incident**

In response to the incident, Woodloch Properties has changed passwords to user accounts and tightened endpoint monitoring controls, among other measures. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through TransUnion.

### **4. Contact information**

Woodloch Properties takes the security of the information in its control seriously and is committed to ensuring information within its control is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a horizontal line extending to the right.

Jason Schwent  
Senior Attorney

cc: Sunaina Ramesh

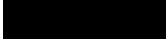
Woodloch Pines and the Lodge at Woodloch  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998

EXHIBIT A



October 18, 2024

## NOTICE OF DATA SECURITY INCIDENT

Dear 

Woodloch Pines and the Lodge at Woodloch (collectively “Woodloch Properties”) experienced a data security incident that may have impacted some of your personal information. We may have your personal information if you have previously visited or stayed at or with Woodloch Properties. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

### What Happened?

On or around May 4, 2024, we identified suspicious activity within the Woodloch Properties network. We immediately disconnected our systems, began an investigation, and engaged independent computer forensic experts to assist. The investigation determined that an unauthorized individual gained access to our systems for a limited period of time. The investigation also determined that files within the systems were accessed during the period of unauthorized access. We then reviewed the contents of the impacted files, and on October 3, 2024, determined that personal information was potentially accessed. While we have no evidence that your particular information was misused, we are making you aware of this incident out of an abundance of caution.

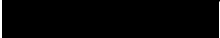
### What Information Was Involved?

From our review, it appears that your name, date of birth, and Social Security number may have been affected.

### What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have changed passwords to user accounts and tightened endpoint monitoring controls, among other measures. In addition, although there has been no evidence your information was misused, we are offering 12 months of complimentary credit monitoring and identity theft protection services through Cyberscout, a TransUnion company.

### What You Can Do:

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: . 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.

000010102G0400

P

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. 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.

**For More Information:**

Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you. If you have questions, please call 1-855-577-9017 Monday to Friday from 8:00 am EST to 8:00 pm EST.

Sincerely,

Woodloch Properties

## Recommended Steps to help Protect your Information

**1. Website and Enrollment.** 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 12 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.

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:  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.

**2. Activate the credit monitoring** provided as part of your Cyberscout, a TransUnion company membership. **The monitoring included in the membership 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, a TransUnion company will be able to assist you.

**3. Telephone.** Contact Cyberscout, a TransUnion company at 1-855-577-9017.

**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](http://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.

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](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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.



00001020280000

P

**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](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://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](http://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/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.

**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](http://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/](http://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](http://www.riag.ri.gov), Telephone: 401-274-4400. A total of [XX] Rhode Island residents were notified of this incident.

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