



Todd M. Rowe, Partner
Cybersecurity & Data Privacy Team
20 North Wacker, Suite 4120
Chicago, IL 60606
TRowe@constangy.com
Mobile: 773.558.2363

January 21, 2025

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: Idtheft@oag.state.md.us

RE: Notice of Data Security Incident

To Attorney General Brown:

We represent Columbia Hospitality ("Columbia") in connection with a recent data security incident described below. Columbia is notifying affected individuals of the incident. The purpose of this letter is to provide formal notice to your office pursuant to Md. Code Ann., Comm. Law § 14-3504.

I. Nature of the Security Incident

On July 30, 2024, Columbia experienced an incident disrupting computer network operations. Upon discovery, Columbia took immediate steps to secure the environment. In addition, Columbia retained an independent computer forensic investigator to conduct an investigation to determine what happened. The forensic investigation revealed that an unauthorized actor gained access to the Columbia network, and that some personal information may have been acquired without authorization in connection with the incident. Columbia thereafter undertook a comprehensive review to determine what information may have been impacted, the individuals to whom the information pertained, the addresses for those individuals, and worked diligently to provide notice to affected individuals.

II. Number of Maryland Residents Notified

Columbia's investigation determined that the information affected for Maryland residents may have included name and Social Security number. Columbia notified six (6) Maryland residents of this incident by sending notification letters via first class U.S. mail on January 17, 2025. A sample copy of that notification letter is enclosed.

III. Actions Taken in Response to the Incident

As soon as Columbia discovered this incident, it launched an investigation, took immediate steps to enhance the security of its network, and worked to determine whether any personal information was accessed or acquired without authorization. Columbia then worked diligently to determine what personal information may have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification. Columbia has additionally notified the FBI of the incident, and will cooperate with any resulting investigation.

Attorney General Anthony G. Brown
January 21, 2025

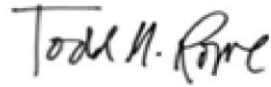
Constangy, Brooks, Smith & Prophete, LLP

As part of the notice, Columbia is offering Maryland residents whose Social Security numbers may have been affected 12 months of credit monitoring and Cyberscan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 773.558.2363 or trowe@constangy.com.

Sincerely,

A handwritten signature in black ink that reads "Todd N. Rowe". The signature is written in a cursive, slightly slanted style.

Todd Rowe
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Encl. Sample Consumer Notice Letter

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

January 17, 2025

Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident that may have affected your personal information. Columbia Hospitality and one of its managed properties, Semiahmoo Resort, (“Columbia”) takes the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On July 30, 2024, Columbia became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain Columbia data may have been acquired without authorization on or about July 30, 2024. As a result, Columbia undertook a review of the potentially affected files. Our review concluded on December 10, 2024, and identified that some of your information may have been involved. Since that time, we have been working to gather contact information needed to provide you with this notice.

What Information Was Involved. The potentially affected information may have included your <<Variable Text 2>>.

What We Are Doing. As soon as Columbia discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<Membership Offering Length>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (877) 719-8145, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note, the deadline to enroll is April 17, 2025

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. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

Please call (877) 719-8145 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Brian Flaherty
Chief Executive Officer of Columbia Hospitality

Columbia Hospitality
2200 Alaskan Way
Ste 200
Seattle, WA 98121

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection 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, IDX will be able to assist you.

3. 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 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.

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.

4. 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.

5. 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.

6. 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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/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, 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: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

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