LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsey Smith
100 Light Street, Suite 1300
Baltimore, Maryland 21202
Lindsey.Smith@lewisbrisbois.com
Direct: 410.525.6402

February 2, 2022

File No. 44629.124

VIA E-MAIL

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

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

I represent Concord Hospitality Enterprises Company, LLC ("Concord") located in Raleigh, NC, with respect to a recent data security incident described in greater detail below. Concord takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the Security Incident.

On August 24, 2021, Concord experienced a data security incident that prevented employees from accessing internal systems and data. Upon discovering this incident, Concord immediately launched an investigation and engaged a digital forensics firm to help determine what happened and what information may have been accessed. Concord also reported the incident to the Federal Bureau of Investigation. Through its investigation, Concord identified unauthorized access to certain data in its systems. Concord then retained third-party professionals to review the data to identify any personal information that may have been impacted. On January 13, 2022, Concord identified individuals whose personal information may have been impacted as a result of the incident. The personal information included names, addresses, driver's license numbers, and Social Security numbers.

2. Number of Maryland Residents Affected.

Concord notified 183 residents of Maryland via first class U.S. mail on February 2, 2022. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident.

Concord has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps include working with leading cybersecurity experts to enhance the security of its systems and data.

4. Contact Information.

Concord remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 410.525.6402 or via email at Lindsey.Smith@lewisbrisbois.com.

Sincerely,

Lindsey Smith of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LS
Encl.: Consumer Notification Letter Template

CONCORD HOSPITALITY ENTERPRISES

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

To Enroll, Please Call:
(833) 325-1786
Or Visit:
https://response.idx.us/concord
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

February 2, 2022

Re: Notification of Data Security Incident

Dear <<FIRST NAME>> <<LAST NAME>>,

I am writing to inform you of a data security incident experienced by Concord Hospitality Enterprises Company, LLC ("Concord"), which may have involved your personal information, and, as a precaution, we are providing information about steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

What Happened? On August 24, 2021, Concord experienced a data security incident that prevented employees from accessing internal systems and data. Upon discovering this incident, Concord immediately launched an investigation and engaged a digital forensics firm to help determine what happened and what information may have been accessed. Concord also reported the incident to the Federal Bureau of Investigation. Through its investigation, Concord identified unauthorized access to certain data in its systems. Although there is no evidence that your personal information was misused, out of an abundance of caution, we are notifying you of the incident and providing information about steps you can take to protect your information.

What Information Was Involved? The information may have included: <<VARIABLE TEXT>>

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our network to reduce the risk of a similar event 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: [12 months / 24 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 enroll in free identity protection services by calling (833) 325-1786 or going https://response.idx.us/concord and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 2, 2022.

Please call (833) 325-1786 or go to https://response.idx.us/concord for assistance or for any additional questions you may have.

For More Information: Further information about how to protect your information appears on the following page. If you have questions or need assistance, please call (833) 325-1786, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. Please have your Enrollment Code ready.

We regret any worry or inconvenience that this may cause you.

Sincerely,

Brian Cornell

Chief Information Officer
Concord Hospitality Enterprises Company, LLC

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 9532	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-800-525-6285
www.transunion.com	**www.experian.com**	**www.equifax.com**

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, D.C. 20580, or online at consumer.ftc.gov and www.ftc.gov/idtheft, or to the Attorney General in your state. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ag.ny.gov	410-528-8662	1-877-566-7226	1-401-274-4400
1-212-416-8433			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.