MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Brian Fox
Office: (267) 930-4777
Fax: (267) 930-4771
Email: bfox@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 13, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

Our office represents Sceptre Hospitality Resources, Inc. ("SHR") located at 1900 W Loop South, Houston, TX 77027. SHR provides central reservation system ("CRS") services to its hotel clients. We write on behalf of the hotels listed below to notify your office of an incident that may affect the security of some personal information relating to eleven (11) New Hampshire residents who made reservations through SHR's CRS platform. These hotels are Endless Summer Resort - Dockside Inn and Suites, Endless Summer Resort – Surfside Inn and Suites, Portofino Bay Hotel, Hard Rock Hotel Orlando, Sapphire Falls Resort, Royal Pacific Resort, Cabana Bay Beach Resort and Aventura Hotel (collectively, the "Hotels"). This notice may be supplemented where additional SHR clients request notice be provided on their behalf. By providing this notice, SHR and the Hotels do not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 28, 2020, SHR discovered suspicious activity related to its CRS. SHR immediately launched an investigation, with the aid of forensic experts, to determine the nature and scope of this incident. SHR determined that, between January 22 and January 29, 2020, there was unauthorized access to guest reservation data maintained on its CRS. SHR undertook a lengthy and labor-intensive process to identify the personal information that may have been accessed. SHR is providing notice to the Hotels and offered to provide notice on their behalf to the appropriate state regulators. The type of personal information related to the affected New Hampshire residents

include the following: name, postal and email address, telephone number and credit card information.

Notice to New Hampshire Residents

The Hotels are providing written notice of this incident to guests affected by the issue. A sample of the letter is attached hereto and labeled as ***Exhibit A***.

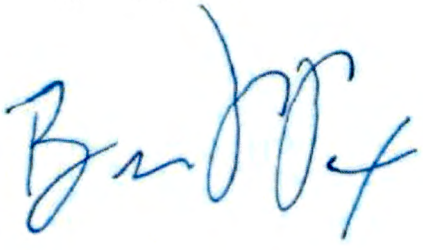
Other Steps Taken and To Be Taken

Upon discovering this incident, SHR immediately launched an investigation to determine the nature and scope of the event, as well as whose data may potentially be affected. As an added precaution, SHR is offering each affected individual twelve months of credit monitoring and identity restoration services at no cost to the individual. SHR has taken steps to ensure the security of the information it stores.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4777.

Very truly yours,



Brian Fox of
MULLEN COUGHLIN LLC

Enclosure

EXHIBIT A

[HOTEL NAME]

[DATE]

[AFFECTED INDIVIDUAL NAME AND ADDRESS]

Dear **[name of affected individual]**:

We are writing to inform you of an issue involving the reservation information you gave us when you arranged your stay at <**hotel name**>. The issue affected the systems of Sceptre Hospitality Resources ("SHR"), a service provider we use to manage your reservation. It did not affect our own systems.

SHR recently informed us that, between January 22 and January 29, 2020, an unauthorized party gained access to guest reservation data for a limited number of guests whose information was maintained on SHR's systems. SHR has indicated that the affected reservation information may have included guests' names; contact information; payment card information, including cardholder name, payment card number, expiration date and security code; and other booking information entered at the time of reservation.

We are taking this matter very seriously. The protection of our guest data is a top priority for us. After learning of the issue, we quickly began working with SHR to address the matter and identify our affected guests. We understand that SHR took steps to secure its systems and stop the unauthorized access to its systems. SHR also has engaged an outside firm to conduct a forensic investigation and contacted law enforcement authorities. The relevant payment card brands also have been notified of the issue. As indicated above, this issue occurred on SHR's systems and did not impact our systems.

We take our obligation to safeguard our guests' information very seriously and are alerting you about this issue so you can take steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. In addition, we have arranged to offer credit monitoring and identity restoration services to affected guests for one year at no cost to those guests. The enclosed Reference Guide provides information on these services and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We regret that this issue at SHR may affect you and hope this information is useful to you. If you have any questions regarding this issue, please contact **[relevant toll-free number of call center]**.
Sincerely,

[Name and title of hotel signatory]

Reference Guide

We encourage affected guests to take the following steps:

Register for Credit Monitoring and Identity Restoration Services. We have arranged with TransUnion Interactive to offer you credit monitoring services and identity restoration services for one year at no cost to you. You can sign up for these services online or via U.S. mail delivery, as described below.

- To enroll, go to www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code << **Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode 698691 and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and June 30, 2020. Credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1 million in identity theft insurance with no deductible (policy limitations and exclusions may apply.)

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be

explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to

prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.
The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:
Office of the Attorney General

The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/internet/resource-center

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
http://www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as

a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.