BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

July 9, 2019

VIA OVERNIGHT MAIL

Joseph Foster
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

We are writing on behalf of the Alexandrian Hotel ("Alexandrian"), to notify you of a security incident involving 1 New Hampshire resident.

On June 13, 2019, the Alexandrian learned that a hotel employee inadvertently sent a spreadsheet to a fellow conference attendee that contained some of personal information of hotel guests. The employee realized their mistake immediately and the Alexandrian confirmed with the recipient that the message with the spreadsheet was deleted and not disclosed to any other person. The spreadsheet contained guest information, including name, address, payment card number, and expiration date. The Alexandrian is not aware of any resulting identity theft, fraud, or financial losses to customers.

On June 14, 2019 the Alexandrian notified potentially affected individuals via email. On June 19, 2019, the Alexandrian began mailing written notifications to potentially affected individuals, including 1 New Hampshire resident who is being notified of the incident in writing in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the document enclosed herewith.[1] The Alexandrian has provided a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent something like this from happening in the future, the Alexandrian is reinforcing employee training on the importance of safeguarding personal information.

[1]This report does not waive the Alexandrian's objection that New Hampshire lacks personal jurisdiction over this matter.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

M. Scott Koller

M. Scott Koller
Partner

Enclosure

THE
ALEXANDRIAN
OLD TOWN ALEXANDRIA, VA

AUTOGRAPH COLLECTION®
HOTELS

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

June 19, 2019

Notice of Data Breach

Dear <<Name 1>>:

At the Alexandrian Hotel, we value the relationship we have with our guests and understand the importance of protecting personal information. We are writing to inform you that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, measures we have taken in response, and some additional steps you may consider taking.

What Happened?
On June 13, 2019, we learned that a Hotel employee inadvertently sent a spreadsheet to a fellow conference attendee that contained some of your personal information. The employee realized their mistake immediately we confirmed with the recipient that the message was deleted.

What Information Was Involved?
The spreadsheet contained information related to your upcoming stay, including your name, address, payment card number, and the expiration date for the card ending in <<Last 4 of Card Number>>.

What We Are Doing.
We have confirmed with the agent that the spreadsheet was deleted and not disclosed to any other person. To help prevent something like this from happening in the future, we are reinforcing employee training on the importance of safeguarding personal information.

What You Can Do.
Although we have no reason to believe your information has or will be misused, we wanted to let you know about this incident and assure you that we take it very seriously. It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized credit card charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

For More Information.
We regret that this incident occurred and apologize for any inconvenience. If you have questions regarding this incident, you can call 703-842-2777 during normal business hours.

Sincerely,

Michael Nelson
General Manager

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

If you are a resident of Maryland or North Carolina, or you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors

and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.