BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

November 29, 2019

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident

Dear Attorney General MacDonald:

We are writing on behalf of our client, Choice Hotels International, Inc. ("Choice"), to notify your office of a security incident involving New Hampshire residents. Choice is located at 1 Choice Hotels Circle, Suite 400, Rockville, Maryland 20850.

Choice recently learned of a technical issue that only occurred in a specific circumstance. The cause of the issue has been addressed. The issue involved information entered by a visitor to Choice's website being inadvertently accessible to third parties, with whom Choice has a business relationship, when the visitor's web browser crashed while on the site. Choice uses technology to track activities that occur on its website (e.g., cookies), and that technology sends data to companies that provide services to Choice. For visitors to Choice's website who used the Safari web browser, if Safari crashed and restarted, Safari would put information that had been typed by the visitor on the page into the website address for that page. Tracking technology reads the website address of pages on Choice's website and sends the data to third parties. Except in a Safari crash circumstance, the page address does not contain information entered by visitors. Choice believes this occurred because of how the code for Safari was written. This specific issue occurred approximately 88,000 times from June 2015 through November 12, 2019.

If a visitor to Choice's website was using Safari and on the reservation page, the information that had been typed in fields on that page that could have been put in the website address when the browser restarted after a crash may include the name of the person making the reservation, email address, state, zip code, country code, and the number and expiration date of the payment card used to make the reservation. If the individual making the reservation was using a

mixture of points and payment, the external verification value on the card may have also been in the website address.

Today, Choice is providing substitute notification to the New Hampshire residents involved in the incident. Choice was able to identify the guest reservations made since April 2016 that were involved in the incident and the email addresses for those reservations. Choice will be sending notice via email to the 285 New Hampshire residents in that group. Choice believes that this scenario occurred very infrequently from June 2015 to March 2016 (likely less than 25 times), but it does not have information available to identify the specific guests, so Choice is issuing a press release and is posting a statement on its website to provide notice to those individuals. Copies of the email notification, press release, and website statement are attached.

As soon as Choice identified the scenario that caused this on November 12, 2019 following a call from a customer, Choice made changes to the code that operates its website to override how Safari responds after a crash. Choice is also contacting the third-party companies it works with to ask them to delete any data they may have.

Sincerely,

Craig A. Hoffman
Partner

Attachment

[header – translation links]

German (Deutsch) | Spanish (Espana) | Spanish (Latinoamerica) | French (Canadien) | French (Francais) | Dutch (Nederlands) | Norwegian (Norsk) | Swedish (Svenska)

Notice of Data Breach

Dear Valued Guest:

Choice Hotels understands the importance of data security, and protecting guest information is a priority. We are writing to notify you of an inadvertent disclosure issue involving some of your information and what we have done in response.

What Happened?
Choice recently learned of a technical issue that only occurred in a specific circumstance. The cause of the issue has been addressed. The issue involved information entered by a visitor to Choice's website being inadvertently accessible to third parties, with whom Choice has a business relationship, when the visitor's web browser crashed while on the site. Choice uses technology to track activities that occur on its website (e.g., cookies), and that technology sends data to companies that provide services to Choice. For visitors to Choice's website who used the Safari web browser, if Safari crashed and restarted, Safari would put information that had been typed by the visitor on the page into the website address for that page. Tracking technology reads the website address of pages on Choice's website and sends the data to third parties. Except in a Safari crash circumstance, the page address does not contain information entered by visitors. We believe this occurred because of how the code for Safari was written. This specific issue occurred approximately 88,000 times from June 2015 through November 12, 2019.

What Information Was Involved?
If a visitor to Choice's website was using Safari and on the reservation page, the information that had been typed in fields on that page that could have been put in the website address when the browser restarted after a crash may include the name of the person making the reservation, email address, state, zip code, country code, and the number and expiration date of the payment card used to make the reservation. We are notifying you because this scenario occurred when you were making a reservation. If you were making a reservation using a mixture of points and payment, the external verification value on the card may have also been in the website address. The last four digits of the card you used were [wxyz].

What We Are Doing.
As soon as we identified the scenario that caused this on November 12, 2019, Choice made changes to the code that operates our website to override how Safari responds after a crash. We are also contacting the third-party companies we work with to ask them to delete any data they may have.

What You Can Do.
Although the issue was due to a technical issue and not as a result of an unauthorized party trying to obtain this data, it is always advisable to monitor your payment card account statements for unauthorized charges. You should immediately report any unauthorized charges to the bank that issued your card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card. It is also a good idea to be wary of unsolicited email, text messages, or mail.

For More Information.
We regret that this occurred and apologize for any inconvenience. If you have any questions, please contact our Data Protection Officer at dpo@choicehotels.com.

ADDITIONAL INFORMATION

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

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

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *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, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov
- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Rhode Island, note that pursuant to Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

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 one (1) year. 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 hour 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 hour 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.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Choice Hotels International, Inc., One Choice Hotels Circle, Suite 400, Rockville, MD 20850

[header – translation links]

German (Deutsch) | Spanish (Espana) | Spanish (Latinoamerica) | French (Canadien) | French (Francais) | Dutch (Nederlands) | Norwegian (Norsk) | Swedish (Svenska)

Notice of Data Breach

November 29, 2019

Choice Hotels understands the importance of data security, and protecting guest information is a priority. We are notifying guests of an inadvertent disclosure issue involving some of their information and what we have done in response.

What Happened?
Choice recently learned of a technical issue that only occurred in a specific circumstance. The cause of the issue has been addressed. The issue involved information entered by a visitor to Choice's website being inadvertently accessible to third parties, with whom Choice has a business relationship, when the visitor's web browser crashed while on the site. Choice uses technology to track activities that occur on its website (e.g., cookies), and that technology sends data to companies that provide services to Choice. For visitors to Choice's website who used the Safari web browser, if Safari crashed and restarted, Safari would put information that had been typed by the visitor on the page into the website address for that page. Tracking technology reads the website address of pages on Choice's website and sends the data to third parties. Except in a Safari crash circumstance, the page address does not contain information entered by visitors. We believe this occurred because of how the code for Safari was written.

This specific issue occurred approximately 88,000 times from June 2015 through November 12, 2019. Choice identified the guest reservations involved that occurred since April 2016 and has sent emails to those guests. We believe that this scenario occurred very infrequently from June 2015 – March 2016 (likely less than 25 times), but we do not have information available to identify the specific guests so we are issuing a press release and posting this notice to notify those guests.

What Information Was Involved?
If a visitor to Choice's website was using Safari and on the reservation page, the information that had been typed in fields on that page that could have been put in the website address when the browser restarted after a crash may include the name of the person making the reservation, email address, state, zip code, country code, and the number and expiration date of the payment card used to make the reservation. We are notifying you because this scenario occurred when you were making a reservation. If you were making a reservation using a mixture of points and payment, the external verification value on the card may have also been in the website address.

What We Are Doing.
As soon as we identified the scenario that caused this on November 12, 2019, Choice made changes to the code that operates our website to override how Safari responds after a crash. We are also contacting the third-party companies we work with to ask them to delete any data they may have.

What You Can Do.
Although the issue was due to a technical issue and not as a result of an unauthorized party trying to obtain this data, it is always advisable to monitor your payment card account statements for

unauthorized charges. You should immediately report any unauthorized charges to the bank that issued your card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card. It is also a good idea to be wary of unsolicited email, text messages, or mail.

For More Information.
We regret that this occurred and apologize for any inconvenience. If you have any questions, please contact our Data Protection Officer at dpo@choicehotels.com.

ADDITIONAL INFORMATION

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

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

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *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
- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts and Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

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 one (1) year. 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 hour 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 hour 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.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Choice Hotels International, Inc., One Choice Hotels Circle, Suite 400, Rockville, MD 20850

[press release – PRNewsire national US distribution]

Choice Hotels Notifies Guests of Inadvertent Disclosure Issue

ROCKVILLE, Md., Nov. 29, 2019 /PRNewswire/ -- Choice Hotels International, Inc. (NYSE: CHH), has taken steps to address and notify guests of an issue involving inadvertent disclosure of certain guest information to third parties with whom Choice has business relationships. While most guests involved have been contacted already, the company is issuing this press release to alert the small number it could not identify. The issue occurred very infrequently from June 2015 – March 2016 (likely less than 25 times), but information to identify specific guests involved during this timeframe is unavailable. Overall, this issue occurred approximately 88,000 times from June 2015 through November 12, 2019, and Choice has already notified individuals involved from April 2016 forward by sending them an email.

Choice Hotels understands the importance of data security, and protecting guest information is a priority. The company recently learned of a technical issue that only occurred when a visitor to its website was using a Safari browser, typed information in a field on the page, and the browser crashed and restarted. Under these circumstances, Safari put information that had been typed by the visitor on the page into the website address in order to repopulate the page when the browser restarted. Choice uses technology to track activities that occur on its website (e.g., cookies), and that technology sends data read from the website address of relevant pages to companies that provide services to it. Except in a Safari crash circumstance, the page address sent to these companies did not contain information entered by visitors.

As soon as Choice identified what caused this issue, the company made changes to its website to override how Safari responds after a crash. Choice is also contacting the third-party companies it works with to ask them to delete any data they may inadvertently have.

What Information Was Involved?
If a visitor was using Safari and was on the reservation page when the browser crashed, the information typed in fields on that page that could have been put in the website address when the browser restarted may include the name of the person making the reservation, email address, state, zip code, country code, and the number and expiration date of the payment card used to make the reservation. If the reservation was being made using a mixture of points and payment, the external verification value on the card may have also been in the website address.

For More Information.
Please visit www.choicehotels.com/about/browser-crash-incident for additional information.