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

October 12, 2017

VIA OVERNIGHT MAIL

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

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Hyatt Hotels Corporation ("Hyatt") to notify you of a security incident involving New Hampshire residents.[1]

On July 7, 2017, Hyatt identified suspicious activity on one of its corporate servers. Upon discovery, Hyatt launched a comprehensive investigation to identify what happened and how it occurred, including engaging leading third-party experts, payment card networks and authorities. Findings from the recently completed investigation determined that there was unauthorized access to payment card information from cards manually entered or swiped at the front desk of certain Hyatt-managed and franchised locations between March 18, 2017 and July 2, 2017. The information that was involved includes cardholder names, card numbers, expiration dates and internal verification codes (CVVs).

The available data and information did not enable Hyatt to identify the specific payment cards that may have been affected. Out of an abundance of caution, beginning today, October 12, 2017, Hyatt, on its behalf and for those managed and franchised locations that are involved, is notifying all individuals who used payment cards at the identified Hyatt locations during the relevant time period, including 28 New Hampshire residents, in substantially the same form as the attached letter. Notification is being made as soon as possible in accordance with N.H. Rev. Stat. § 359-C:20. In addition, Hyatt has set up a call center staffed with dedicated support specialists

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

that potentially affected individuals can call to have their questions answered. Hyatt is also reminding potentially affected individuals to review their account statements and credit reports for any indicators of fraud.

Over time, Hyatt has implemented enhanced cybersecurity measures and additional layers of defense which helped to identify and resolve the unauthorized access. Hyatt is continuing to evaluate its security measures and processes to identify where additional improvements are necessary to help prevent a similar incident from happening in the future.

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

Sincerely,

Craig A. Hoffman
Partner

Enclosure

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear Hyatt Guest,

We understand the importance of protecting customer information and securing our systems, and we regret to inform you that we self-discovered signs of and resolved unauthorized access to payment card information from cards manually entered or swiped at the front desk of certain Hyatt-managed locations between March 18, 2017 and July 2, 2017.

Upon discovery, we launched a comprehensive investigation to understand what happened and how this occurred, including engaging leading third-party experts, payment card networks and authorities. Our enhanced cybersecurity measures and additional layers of defense implemented over time helped to identify and resolve the issue. I want to assure you that there is no indication that information beyond that gained from payment cards – cardholder name, card number, expiration date and internal verification code – was involved, and as a result of measures we have taken to prevent this from happening in the future, guests can feel confident using payment cards at Hyatt hotels worldwide.

We estimate that the incident affected a small percentage of payment cards used by guests who visited the group of affected Hyatt hotels during the at-risk time period, but the available information and data does not allow Hyatt to identify the specific payment cards that may have been affected. It's important to Hyatt that we notify our guests and provide helpful information about steps you can take, and you are receiving this communication because you have been identified as a guest who checked in to an affected hotel during the at-risk time period. As always, the primary step customers can take is to review their payment card account statements closely and report any unauthorized charges to their card issuer immediately.

This incident is something we take seriously, and we are sorry for the inconvenience and concern this may cause you. For frequently asked questions and a list of affected hotels and respective at-risk dates, please visit hyatt.com/protectingourcustomers. If you have questions or would like more information, please call +1-855-474-9288 (English) or +1-402-938-3421 (Spanish/English) from 7:00 a.m. to 9:00 p.m. CST.

Sincerely,

Chuck Floyd
Global President of Operations
Hyatt Hotels Corporation

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain 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, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
(410) 576-6300 (for calls originating outside Maryland)

Office of the Attorney General, One Ashburton Place, Boston, MA 02108, 1-508-990-8686, www.mass.gov/ago/contact-us.html

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400

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

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

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 may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

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

In order 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 (5) 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 three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail 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 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail 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 three (3) business days after receiving your request to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- 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. And 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 may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.