

BakerHostetler

Baker & Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212.271.1504
tkobus@bakerlaw.com

November 30, 2018

**VIA E-MAIL (CONSUMER@IOWA.GOV)
AND OVERNIGHT MAIL**

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319

Re: Incident Report

Dear Sir or Madam:

I am writing on behalf of our client, Marriott International, Inc. ("Marriott"), to report an incident involving Iowa residents.

On September 8, 2018, Marriott¹ received an internal alert regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

Marriott has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also

¹ Marriott completed its acquisition of Starwood Hotels & Resorts Worldwide, Inc. ("Starwood") in September 2016. Starwood operates on a separate computer network from Marriott.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components of information needed to decrypt the numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and, sometimes, other data, such as mailing address, email address, or other information. Marriott is working to determine the number of Iowa residents whose information was in the database.

On November 30, 2018, Marriott will begin² sending emails to guests whose information was in the Starwood guest reservation database notifying them of the incident. A copy of the notification is enclosed. Today Marriott also released a statement to media outlets nationwide, and posted notice on the Starwood website, available at info.starwoodhotels.com. These notices meet the substitute notice requirements of Iowa Code § 715C.2(4)(c). Marriott is also providing a telephone number for potentially affected individuals to call with any questions they may have. The website notice and call center are each available in fifteen languages to support Marriott's diverse guest population.

Marriott is also providing eligible guests the opportunity to enroll in WebWatcher free of charge for one year. WebWatcher monitors internet sites where personal information is shared and generates an alert to the consumer if evidence of the consumer's personal information is found. Guests from the United States who complete the WebWatcher enrollment process will also be provided fraud consultation services and reimbursement coverage for free.

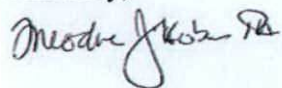
The Starwood network had administrative, technical, physical, and logical security measures in place, including an IBM database monitoring tool. An alert from the tool caused Marriott to investigate the Starwood network. Marriott has taken, and continues to take, significant steps to help prevent this type of incident from happening again. Marriott installed an endpoint security tool (CrowdStrike Falcon) on devices across the Starwood network during the investigation, which actively monitors the device and generates alerts, and has a next-generation antivirus prevention feature. Malicious files and tools installed during the incident have been blocked or removed by security tools. Additional security enhancements were added including enhanced logging and monitoring, further segmentation, and expanded multi-factor authentication, as well as password resets and vulnerability scanning. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to its network. Marriott reported this incident to law enforcement and continues to support their investigation.

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

² Marriott is sending emails to involved guests as quickly as possible while trying to ensure sufficient call center support for those who receive notice on a daily basis.

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
November 30, 2018
Page 3

Sincerely,

A handwritten signature in black ink, appearing to read "Theodore J. Kobus III". The signature is written in a cursive, flowing style with a large initial "T" and "K".

Theodore J. Kobus III
Partner

Enclosure

From: Starwood Hotels <starwoodhotels@email-marriott.com>

Sent: Friday, November 30, 2018

To:

Subject: Starwood Guest Reservation Database Security Incident



[California Residents](#) | [California - Español](#)
[العربية](#) | [中文](#) | [简体中文](#) | [Deutsch](#) | [Español \(España\)](#) | [Español \(Latinoamérica\)](#)
[Français \(Canadien\)](#) | [Français](#) | [Italiano](#) | [日本人](#) | [Português \(Europeu\)](#) |
[Português \(Brasil\)](#)
[한국어](#) | [Русский](#)

Dear Valued Guest,

Marriott values our guests and understands the importance of protecting your personal information. We have taken measures to investigate and address a data security incident involving the Starwood guest reservation database. The investigation has determined that there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties* on or before September 10, 2018. This notice explains what happened, measures we have taken, and some steps you can take in response.

Starwood Guest Reservation Database Security Incident

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

Marriott has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information.

Marriott reported this incident to law enforcement and continues to support their investigation. The company is also notifying regulatory authorities.

Marriott deeply regrets this incident happened. From the start, we moved quickly to contain the incident and conduct a thorough investigation with the assistance of leading security experts. Marriott is working hard to ensure our guests have answers to questions about their personal information with a dedicated website and call center. We are supporting the efforts of law enforcement and working with leading security experts to improve. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing

security enhancements to our network.

Guest Support

Marriott has taken the following steps to help you monitor and protect your information:

Dedicated Call Center

Marriott has established a dedicated call center to answer questions you may have about this incident. The call center is open seven days a week, and is available in multiple languages. Our dedicated call center may experience high volume initially, and we appreciate your patience.

Email notification

Marriott began sending emails on a rolling basis on November 30, 2018 to affected guests whose email addresses are in the Starwood guest reservation database.

Free WebWatcher Enrollment

Marriott is providing guests the opportunity to enroll in WebWatcher free of charge for one year. WebWatcher monitors internet sites where personal information is shared and generates an alert to the consumer if evidence of the consumer's personal information is found. Due to regulatory and other reasons, WebWatcher or similar products are not available in all countries. Guests from the United States who complete the WebWatcher enrollment process will also be provided fraud consultation services and reimbursement coverage for free.

The section below provides additional information on steps you can take. If you have questions about this notification and to enroll in WebWatcher (if it is available in your country), please visit info.starwoodhotels.com.

* Starwood brands include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels. Starwood branded timeshare properties are also included.

Best wishes,



Arne Sorenson

MORE INFORMATION ON STEPS YOU CAN TAKE

Regardless of where you reside, below are some additional steps you can take.

- Monitor your SPG account for any suspicious activity.
- Change your password regularly. Do not use easily guessed passwords. Do not use the same passwords for multiple accounts.
- Review your payment card account statements for unauthorized activity and immediately report unauthorized activity to the bank that issued your card.
- Be vigilant against third parties attempting to gather information by deception (commonly known as "phishing"), including through links to fake websites. Marriott will not ask you to provide your password by phone or email.
- If you believe you are the victim of identity theft or your personal data has been misused, you should immediately contact your national data protection authority or local law enforcement.

If you are a resident of the United States:

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, www.ct.gov/ag, 1-860-808-5318

Maryland Attorney General's Office, 200 St. Paul Place,
Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or
1-410-576-6300

Office of the Massachusetts Attorney General, One Ashburton
Place, Boston, MA 02108, www.mass.gov/ago/contact-us.html,
1-617-727-8400

North Carolina Attorney General's Office, 9001 Mail Service
Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or
1-877-566-7226

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

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 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 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 number 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 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 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.

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 are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are 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. You must give your consent for reports to be provided to employers.
 - You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
 - You may seek damages from violators.
 - Identity theft victims and active duty military personnel have additional rights.

If You Are A European Union Data Subject, you may contact or obtain information from your Data Protection Authority at:

Austria: Österreichische Datenschutzbehörde,
Wickenburggasse 8, 1080 Vienna, +43 1 52 152 0, Email:
dsb@dsb.gv.at

Belgium: De Gegevensbeschermingsautoriteit (GBA), Rue de la
Presse 35, 1000 Brussels, +32 (0)2 274 48 00, Email:
contact@apd-gba.be

Bulgaria: Commission for Personal Data Protection (CPDP), 2
Prof. Tsvetan Lazarov Blvd., Sofia 1592, +359 899 877 156,
Email: kzld@cpdp.bg

Croatia: Croatian Personal Data Protection Agency (AZOP), Fra
Grge Martica 14, HR-10 000 Zagreb, +385 (0)1 4609-000,
Email: azop@azop.hr

Cyprus: Office of the Commissioner for Personal Data
Protection, Iasonos 1, 1082 Nicosia (office address), P.O. Box
23378, 1682 Nicosia, Cyprus (postal address), +357 22818456,
Email: commissioner@dataprotection.gov.cy

Czechia (Czech Republic): The Office for Personal Data
Protection, Pplk. Sochora 27, 170 00 Praha 7, +420 234 665
111, Email: posta@uoou.cz

Denmark: Datatilsynet, Borgergade 28, 5, 1300 København,
+45 33 19 32 00 (Monday – Thursday 9:00am to 12:00pm and

12:30 to 3:30pm, Friday 9:30am to 12:00pm), Email:
dt@datatilsynet.dk

Estonia: Andmekaitse Inspektsioon, 19 Väike-Ameerika St.,
10129 Tallinn, +372 627 4135, Email: info@aki.ee

Finland: Tietosuojavaltuutetun toimisto, Ratapihantie 9, 6th
Floor, 00520, Helsinki (office address), P.O. Box 800, 00521
Helsinki (postal address), +358 29 566 6700, Email (registry):
tietosuoja@om.fi

France: Commission nationale de l'informatique et des libertés
(CNIL), 3 Place de Fontenoy TSA 80715, 75334 PARIS CEDEX
07, +33 01 53 73 22 22 (Monday to Thursday 9:00am to
6:30pm, Friday 9:00am to 6:00pm)

Germany: Die Bundesbeauftragte für den Datenschutz und die
Informationsfreiheit (BfDI), Husarenstr. 30 - 53117 Bonn, +49
(0)228-997799-0, Email: poststelle@bfdi.bund.de. (You may
also contact the Data Protection Agency in your Bundesland.)

Greece: Data Protection Authority Offices, Kifissias 1-3, 115 23
Athens, +30-210 6475600, Email: contact@dpa.gr

Hungary: Nemzeti Adatvédelmi és Információszabadság
Hatóság, H-1125 Budapest, Szilágyi Erzsébet fasor 22/C, +36 1
391 1400, Email: privacy@naih.hu

Ireland: Data Protection Commission (Comisiún Cosanta
Sonraí), Canal House, Station Road, Portarlinton, R32 AP23
Co. Laois, +353 57 868 4800, +353 (0761) 104 800, Email:
info@dataprotection.ie

Italy: Garante per la protezione dei dati personali, Piazza
Venezia 11 – 00187 Roma, +39 06 6967 71, +39 06 6967
72917, Email: urp@gpdp.it

Latvia: Data State Inspectorate, Blaumana Street 11 / 13–11,
Riga, LV–1011, +371 67 22 31 31 (1:00 to 3:00pm), Email:
info@dvi.gov.lv

Lithuania: Valstybine duomenų apsaugos inspekcija, A.
Juozapaviciaus g. 6, 09310 Vilnius 6, 09310 Vilnius, +370 (8 5)
271 2804, 279 1445, Email: paštas ada@ada.lt

Luxembourg: Commission Nationale Pour La Protection Des
Données (CPND), 1, avenue du Rock'n'Roll, L-4361 Esch-sur-
Alzette, +352 26 10 60 – 1

Malta: Office of the Information and Data Protection
Commissioner (IDPC), Level 2, Airways House, High Street,
Sliema SLM 1549, +356 2328 7100, Email:
idpc.info@idpc.org.mt

Netherlands: Autoriteit Persoonsgegevens, Postbus 93374,
2509 AJ DEN HAAG, +31 (0)70 888 85 00

Poland: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-
193 Warszawa, +48 22 531 03 00, Email:
kancelaria@uodo.gov.pl

Portugal: Comissão Nacional de Protecção de Dados (CNPd),
Av. D. Carlos I, 134 - 1.º, 1200-651 Lisboa, +351 21 392 84 00,
Email: geral@cnpd.pt

Romania: Autoritatea Nationala de Supraveghere a Prelucrării
Datelor cu Caracter Personal (ANSPDCP), 28-30 G-ral
Gheorghe Magheru Bld., District 1, post code 010336,
Bucharest, +40 318 059 211, Email: presa@dataprotection.ro,
anspdcip@dataprotection.ro

Slovakia: Úrad na ochranu osobných údajov, Hranicná 12, 820
07, Bratislava 27, +421 2 32313214, Email:
statny.dozor@pdp.gov.sk

Slovenia: Informacijski pooblaščenec, Dunajska cesta 22, SI-
1000 Ljubljana, +386 1 230 97 30, Email: gp.ip@ip-rs.si

Spain: Agencia Española de Protección de Datos (AEPD),
Jorge Juan, 6, 28001 Madrid, +34 913 996 207, Email:

contratacion@agpd.es

Sweden: Datainspektionen, Box 8114, 104 20 Stockholm, +46 08 657 61 00 (Monday, Tuesday, Thursday, Friday: 9:00 to 11:00am; Wednesday: 9:30 to 11:30am), Email: datainspektionen@datainspektionen.se

United Kingdom: Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, +44 0303 123 1113, +44 01625 545 745, Email: dataprotectionfee@ico.org.uk

[TERMS & CONDITIONS OF THE SPG PROGRAM](#) [TERMS OF USE](#) [PRIVACY POLICY](#)

©2018 Marriott International, Inc. All Rights Reserved. Starpoints, SPG, Preferred Guest, Sheraton, Westin, St. Regis, The Luxury Collection, W, Le Méridien, Tribute Portfolio, Element, Aloft, Four Points and their respective logos are the trademarks of Marriott International, Inc., or its affiliates. Design Hotels is a trademark of Design Hotels™.