ROSEWOOD
HOTEL GROUP

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

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

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

We are writing to notify you of an issue that may involve your reservation information. The issue affected the systems of Sabre Hospitality Solutions ("Sabre"), a service provider used by Rosewood Hotel Group ("Rosewood") and other major hotel brands to process guests' hotel reservations. Sabre informed Rosewood that other hotel brands were similarly impacted by this issue. The issue did not affect Rosewood's own systems.

What Happened?

Sabre notified us in late December 2017 that it had uncovered evidence that, between May 29, 2016 and January 11, 2017, an unauthorized party had gained access to certain Rosewood guest reservation information that was maintained on Sabre's systems.

What Information Was Involved?

Sabre has indicated to us that the affected reservation information included guests' names and payment card information (including cardholder name, payment card number, expiration date and security code).

What We Are Doing

After learning of the issue, we quickly began working with Sabre to identify the affected Rosewood guests. We understand that Sabre took steps to disable impacted accounts and stop the unauthorized access to its systems. Sabre also informed us that it engaged an outside cybersecurity expert to conduct a forensic investigation and notified law enforcement authorities. Rosewood notified the relevant payment card brands of the issue. As the service provider that processed the relevant reservation information, Sabre has indicated that it will also notify the relevant payment card brands. As indicated above, this issue occurred on Sabre's systems and did not impact Rosewood's systems.

What You Can Do

We take our obligation to safeguard our guests' information very seriously and we 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. The enclosed Reference Guide provides information on recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We regret that this issue at Sabre may affect you. If you have any questions regarding this issue, please contact 1-844-659-0621, Monday through Friday between 7:00 AM and 7:00 PM Pacific Time. We hope this information is useful to you.

Sincerely,

Symon Bridle
Group Chief Operations Officer
Rosewood Hotel Group

REFERENCE GUIDE

We encourage you to take the following steps:

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. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- 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 Credit Information Services, Inc. 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 19022-2000	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. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

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); and/or
- Proof of your current residential address (such as a current utility bill or account statement).

Website Notice Letter

To Our Valued Guests:

We recently learned of an issue involving unauthorized access to guest information associated with certain hotel reservations at Rosewood Hotel Group ("Rosewood") hotels. The issue affected the systems of Sabre Hospitality Solutions ("Sabre"), a service provider used by Rosewood and other major hotel brands to process guests' hotel reservations. Sabre informed Rosewood that other hotel brands were similarly impacted by this issue. The issue did not affect Rosewood's own systems. If you made a reservation at one of the Rosewood hotels listed here between May 29, 2016 and January 11, 2017, we recommend that you review the information that follows carefully**.**

Sabre notified us in late December 2017 that it had uncovered evidence that, between May 29, 2016 and January 11, 2017, an unauthorized party had gained access to certain Rosewood guest reservation information that was maintained on Sabre's systems. Sabre has indicated to us that the affected reservation information included guests' names and payment card information (including cardholder name, payment card number, expiration date and security code).

After learning of the issue, we quickly began working with Sabre to identify the affected Rosewood guests. We understand that Sabre took steps to disable impacted accounts and stop the unauthorized access to its systems. Sabre also informed us that it engaged an outside cybersecurity expert to conduct a forensic investigation and notified law enforcement authorities. Rosewood notified the relevant payment card brands of the issue. As the service provider that processed the relevant reservation information, Sabre has indicated that it will also notify the relevant payment card brands. As indicated above, this issue occurred on Sabre's systems and did not impact Rosewood's systems.

We regret that this issue at Sabre may affect some of our guests. We take our obligation to safeguard our guests' information very seriously and we are alerting them about this issue so they can take steps to help protect themselves. Affected individuals in the U.S. are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage affected individuals to remain vigilant by reviewing their account statements and monitoring their free credit reports. Please click here for more information and steps affected individuals can take to protect against potential misuse of their information.

If you have any questions regarding this issue, please contact 1-844-659-0621 or 1-503-597-5541, Monday through Friday between 7:00 AM and 7:00 PM Pacific Time.

Sincerely,

Symon Bridle
Group Chief Operations Officer
Rosewood Hotel Group

Reference Guide

We encourage affected individuals to take the following steps:

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. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- 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 Credit Information Services, Inc. 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 19022-2000	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. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

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); and/or
- 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 charge you a fee of up to $5 to place a security freeze on your account, and 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. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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 charge you a fee of up to $10 to place a security freeze on your account, and 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. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

Website FAQs

1. **What happened?**

Rosewood Hotel Group ("Rosewood") was recently informed by Sabre Hospitality Solutions ("Sabre"), a service provider used by Rosewood and other major hotel brands to process guests' hotel reservations, of an issue that affected reservation information for certain Rosewood guests. Sabre informed Rosewood that other hotel brands were similarly impacted by this issue. Sabre notified Rosewood in late December 2017 that it had uncovered evidence that, between May 29, 2016 and January 11, 2017, an unauthorized party had gained access to certain Rosewood guest reservation information that was maintained on Sabre's systems. The issue affected the systems of Sabre and did not affect Rosewood's own systems.

2. **What information was affected by this issue?**

Sabre has indicated to Rosewood that the affected reservation information included guests' names and payment card information (including cardholder name, payment card number, expiration date and security code).

3. **How did Rosewood become aware of the incident?**

Sabre informed Rosewood in late December 2017 of the issue.

4. **Which Rosewood properties were affected?**

Please click here to see a list of the affected Rosewood properties and dates of exposure for each affected hotel.

5. **When did the unauthorized party access payment card information?**

Sabre's investigation found that the unauthorized party first obtained access to Rosewood guests' reservation information on May 29, 2016. The last access to this information by the unauthorized party was on January 11, 2017.

6. **Were Rosewood's systems affected?**

This issue did not affect Rosewood's systems. The issue occurred on the systems of Sabre Hospitality Solutions, a service provider used by Rosewood and other major hotel brands to process guests' hotel reservations. Sabre informed Rosewood that other hotel brands were similarly impacted by this issue.

Rosewood Hotels Properties Affected by the Sabre Hospitality Solutions Issue

Affected Property	Relevant Time Period
Hotel Crescent Court	May 29, 2016 – January 11, 2017
Jumby Bay Resort	June 10, 2016 – January 11, 2017
Las Ventanas al Paraiso A Rosewood Resort	June 3, 2016 – January 11, 2017
Rosewood Abu Dhabi	July 26, 2016 – January 11, 2017
Rosewood Beijing	May 29, 2016 – January 11, 2017
Rosewood Bermuda	June 5, 2016 – January 11, 2017
Rosewood Castiglion del Bosco	June 21, 2016 – January 11, 2017
Rosewood CordeValle	June 2, 2016 – January 11, 2017
Rosewood Hotel Georgia	May 29, 2016 – January 11, 2017
Rosewood Inn of Anasazi	June 3, 2016 – January 11, 2017
Rosewood Mansion on Turtle Creek	June 2, 2016 – January 11, 2017
Rosewood Mayakoba	June 15, 2016 – January 11, 2017
Rosewood London	June 5, 2016 – January 11, 2017
Rosewood Sand Hill	May 31, 2016 – January 11, 2017
Rosewood Washington D.C.	May 31, 2016 – January 11, 2017
The Carlyle: A Rosewood Hotel	May 29, 2016 – January 11, 2017

ROSEWOOD
HOTEL GROUP

NEWS RELEASE January 22, 2018

Security Issue at Sabre Affects Rosewood Guests' Payment Card Information

Rosewood Hotel Group ("Rosewood") announced today an issue affecting certain Rosewood guest reservation information that was maintained on the systems of Sabre Hospitality Solutions ("Sabre"), a service provider used by Rosewood and other major hotel brands to process guests' hotel reservations. Sabre informed Rosewood that other hotel brands were similarly impacted by this issue. The issue occurred on Sabre's systems and did not affect Rosewood's own systems.

Sabre notified Rosewood in late December 2017 that it had uncovered evidence that, between May 29, 2016 and January 11, 2017, an unauthorized party had gained access to certain Rosewood guest reservation information that was maintained on Sabre's systems. Sabre has indicated to Rosewood that the affected reservation information included guests' names and payment card information (including cardholder name, payment card number, expiration date and security code).

After learning of the issue, Rosewood quickly began working with Sabre to identify the affected Rosewood guests. Rosewood understands that Sabre took steps to disable impacted accounts and stop the unauthorized access to its systems. Sabre also informed Rosewood that it engaged an outside cybersecurity expert to conduct a forensic investigation and notified law enforcement authorities. Rosewood notified the relevant payment card brands of the issue. As the service provider that processed the relevant reservation information, Sabre has indicated that it will also notify the relevant payment card brands.

– more –

36/F. NEW WORLD TOWER I. 18 QUEEN'S ROAD CENTRAL. HONG KONG
香港中环皇后大道中18号新世界大厦1期36楼 瑰丽酒店集团
T. +852 2138 2222 电话 F. +852 2138 2233 传真 *rosewoodhotelgroup.com*

ROSEWOOD
HOTEL GROUP

Security Issue at Sabre Affects Rosewood Guests' Payment Card Information - 2

Rosewood takes its obligation to safeguard guests' information very seriously and is alerting them about this issue so they can take steps to help protect themselves. Rosewood encourages guests to carefully review their account statements and monitor their free credit reports for any unauthorized activity. If there is any suspicious or unusual activity, affected individuals should report it immediately to their financial institutions.

Further information for guests, including a list of the properties affected and the dates of exposure for each affected property, can be found online at https://www.rosewoodhotels.com/en/announcement. In addition, guests with questions regarding this incident can call 1-844-659-0621 or +1 503-597-5541 (outside the U.S.), Monday through Friday between 7:00 AM and 7:00 PM Pacific time.

About Rosewood Hotel Group

Rosewood Hotel Group, one of the world's leading hotel companies, encompasses four brands: ultra-luxury Rosewood Hotels & Resorts® in North America, Caribbean/Atlantic, Europe, the Middle East and Asia; contemporary deluxe New World Hotels & Resorts in China and Southeast Asia; neighbourhood lifestyle pentahotels in Europe and Asia; and KHOS™, a dynamic global business lifestyle hotel brand. Its combined portfolio consists of 59 hotels in 18 countries. Rosewood Hotel Group is pursuing a thoughtful expansion strategy with a target of 120 hotels in operation by 2020. For more information, please visit rosewoodhotelgroup.com.

###

For enquiries please contact:

Callie Stanton
Telephone: +1 646 654 3438
Email: cstanton@nikecomm.com