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

March 4, 2016

VIA OVERNIGHT DELIVERY

STATE OF NH
DEPT OF JUSTICE
2016 MAR -7 AM 9:45

Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301-6310

Re: Incident Notification

Dear Attorney General Foster:

Our client, Rosen Hotels & Resorts Inc. (RH&R), recognizes the importance of protecting its customers' payment card data. RH&R received unconfirmed reports on February 3, 2016 of a pattern of unauthorized charges occurring on payment cards after they had been used by some of its guests during their stay. RH&R immediately initiated an investigation into these reports and hired a leading cyber security firm to examine its payment card processing system.

Findings from the investigation show that an unauthorized person installed malware in RH&R's payment card network that searched for data read from the magnetic stripe of payment cards as it was routed through the affected systems. In some instances the malware identified payment card data that included cardholder name, card number, expiration date, and internal verification code. In other instances the malware only found payment card data that did not include cardholder name. No other customer information was involved. Cards used at RH&R between September 2, 2014 and February 18, 2016 may have been affected.

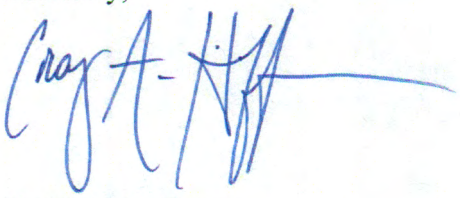
For the approximately 48 New Hampshire residents where the findings show that the payment card information involved included their name and for whom we have a mailing or email address we will be mailing them a letter or sending them an email in accordance with N.H. Rev. Stat. 359-C:19 - C:21 in substantially the same form as the document enclosed herewith. In addition, pursuant to N.H. Rev. Stat. 359-C:19 - C:21, RH&R is providing substitute notification to New Hampshire residents by

posting a statement on its website and issuing a press release in substantially the same form as the documents enclosed herewith. Notice is being provided without unreasonable delay.

RH&R has taken prompt action to resolve this issue and prevent this from happening again. RH&R has also been coordinating its efforts with law enforcement and the payment card networks.

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

Sincerely,



Craig A. Hoffman

Enclosure

Substitute Notice posted as a link at top of www.rosenhotels.com and at each property page with the text of "Payment Card Notice" that links to a page with an address www.rosenhotels.com/protectingourguests that contains the following text:

Rosen Hotels & Resorts Inc. Completes Investigation of Payment Card Incident

March 4, 2016

California residents please click here [embed link]

Rosen Hotels & Resorts Inc. (RH&R) values the relationship we have with our guests and understands the importance of protecting payment card information. We are writing to inform you about an incident that may involve some of that information.

We received unconfirmed reports on February 3, 2016 of a pattern of unauthorized charges occurring on payment cards after they had been used by some of our guests during their stay. We immediately initiated an investigation into these reports and hired a leading cyber security firm to examine our payment card processing system. Findings from the investigation show that an unauthorized person installed malware in RH&R's payment card network that searched for data read from the magnetic stripe of payment cards as it was routed through the affected systems. In some instances the malware identified payment card data that included cardholder name, card number, expiration date, and internal verification code. In other instances the malware only found payment card data that did not include cardholder name. No other customer information was involved. Cards used at RH&R between September 2, 2014 and February 18, 2016 may have been affected.

We are working with the payment card networks to identify the potentially affected cards so that the banks that issued them can be made aware and initiate heightened monitoring on those accounts. For guests where the findings show that the payment card information involved included their name and for whom we have a mailing address or e-mail address, we will be mailing them a letter or sending them an e-mail. We are also supporting law enforcement's investigation.

If you used a payment card at RH&R during this time frame, we recommend that you remain vigilant for signs of unauthorized charges by closely reviewing your payment card account statements. You should immediately report any unauthorized charges to your card issuer 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 your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

Additionally, we have established a dedicated helpline – (855) 907-3214 – if you have questions about this incident. The call center is open from 8 a.m. to 8 p.m. EST, Monday to Friday. Together with our third party cyber security expert, we have worked tirelessly to contain and address the incident. Additional, enhanced security measures have been implemented to help prevent this from happening again. RH&R regrets any inconvenience or concern this may have caused.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and 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 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000, 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. 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

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.

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

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

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

The fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

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, PO Box 740256, Atlanta, GA 30374,www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000,www.transunion.com, 1-800-680-7289

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.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

If you are a resident of West Virginia, you also 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. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374,www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000,www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
(2) Proper identification to verify your identity; and
(3) The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.

Press Release

FOR IMMEDIATE RELEASE

Media Contact: Mary Deatrick
407-718-4640
media@rosenhotels.com

Rosen Hotels & Resorts, Inc. Completes Investigation of Payment Card Incident

Orlando, Fla. – March 4, 2016 – Rosen Hotels & Resorts Inc. (RH&R) values the relationship it has with its guests and understands the importance of protecting payment card information. RH&R received reports on February 3, 2016 of unauthorized charges that occurred on payment cards after they had been used by RH&R guests during their stay. RH&R immediately initiated an investigation into these reports and hired a leading cyber security firm to examine its payment card processing system.

"Together with our cyber security firm, we have worked tirelessly to contain and address the incident. Additional, enhanced security measures have been implemented to help prevent this from happening again," said Frank Santos, Vice President and Chief Financial Officer of Rosen Hotels & Resorts. "We regret the inconvenience and concern this news may cause our customers."

Findings from the investigation show that an unauthorized person installed malware in RH&R's payment card network that searched for data read from the magnetic stripe of payment cards as it was routed through the affected systems. In some instances the malware sought to gather cardholder name, card number, expiration date, and internal verification code from the magnetic stripe on the card, while in other instances the data sought did not include cardholder name. No other customer information was involved. Cards used at RH&R between September 2, 2014 and February 18, 2016 may have been affected.

RH&R is working with payment card networks to identify the potentially affected cards so that the issuing banks can be made aware and initiate heightened monitoring on those accounts. RH&R is also supporting law enforcement's investigation. For guests where the findings show that the payment card information involved included their name and for whom we have a mailing address or e-mail address, RH&R will be mailing them a letter or sending them an e-mail.

RH&R recommends that guests who used a payment card during this time frame remain vigilant for signs of unauthorized charges by closely reviewing their payment card account statements. Guests should immediately report any unauthorized charges to their card issuer 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.

Rosen has established a dedicated helpline – (855) 907-3214 – for guests who have questions about this incident. The helpline is open from 8 a.m. to 8 p.m. EST, Monday to Friday. Guests may also visit www.rosenhotels.com/protectingourguests.

About Rosen Hotels

Celebrating more than 40 years in business, Rosen Hotels & Resorts comprises nearly 6,500 guest rooms at seven Orlando hotels: three convention properties – Rosen Plaza, Rosen Centre and Rosen Shingle Creek, as well as four value-priced leisure properties – Rosen Inn International; Rosen Inn, closest to Universal; Rosen Inn at Pointe Orlando; and Clarion Inn Lake Buena Vista. For more information, visit www.rosenhotels.com.

ROSEN HOTELS & RESORTS
Finance Administration
9840 International Drive • Orlando, FL 32819-8122
tel 407.996.9840 • fax 407.996.6706
RosenHotels.com

March 4, 2016

JANE DOE
123 4TH AVE
APT 5
SEATTLE, WA 67890

Dear JANE DOE:

Rosen Hotels & Resorts Inc. (RH&R) values the relationship we have with our guests and understands the importance of protecting payment card information. We are writing to inform you about an incident that may involve some of that information.

We received unconfirmed reports on February 3, 2016 of a pattern of unauthorized charges occurring on payment cards after they had been used by some of our guests during their stay. We immediately initiated an investigation into these reports and hired a leading cyber security firm to examine our payment card processing system. Findings from the investigation show that an unauthorized person installed malware in RH&R's payment card network that searched for data read from the magnetic stripe of payment cards as it was routed through the affected systems. In some instances the malware identified payment card data that included cardholder name, card number, expiration date, and internal verification code. In other instances the malware only found payment card data that did not include cardholder name. No other customer information was involved. Cards used at RH&R between September 2, 2014 and February 18, 2016 may have been affected.

We are working with the payment card networks to identify the potentially affected cards so that the banks that issued them can be made aware and initiate heightened monitoring on those accounts. For guests where the findings show that the payment card information involved included their name and for whom we have a mailing address or e-mail address, we will be mailing them a letter or sending them an e-mail. We are also supporting law enforcement's investigation.

If you used a payment card at RH&R during this time frame, we recommend that you remain vigilant for signs of unauthorized charges by closely reviewing your payment card account statements. You should immediately report any unauthorized charges to your card issuer 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 your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

Additionally, we have established a dedicated helpline - (855) 907-3214 - if you have questions about this incident. The call center is open from 8 a.m. to 8 p.m. EST, Monday to Friday. Together with our third party cyber security expert, we have worked tirelessly to contain and address the incident. Additional, enhanced security measures have been implemented to help prevent this from happening again. RH&R regrets any inconvenience or concern this may have caused.

Sincerely,

Frank Santos

Frank Santos
Vice-President and Chief Financial Officer
Rosen Hotels & Resorts, Inc.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and 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 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000, 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. 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

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.