

Substitute Notice (Provide a link to the California specific notice imbedded in the Rosen Substitute Notification subpage located on www.rosenhoteles.com)

NOTICE OF DATA BREACH

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

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 your information.

What Happened

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.

What Information Was Involved

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.

What You Can Do

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.

What We Are Doing

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.

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.

For More Information

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. 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.

Press Release

FOR IMMEDIATE RELEASE

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

RE: Notice of a Data Breach

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 your information.

What Happened

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.

What Information Was Involved

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.

What You Can Do

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.

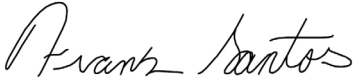
What We Are Doing

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. 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.

For More Information

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. RH&R regrets any inconvenience or concern this may have caused.

Sincerely,

A handwritten signature in cursive script that reads "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.

PAGE LEFT INTENTIONALLY BLANK