Hard Rock Hotel & Casino Las Vegas Notifies Customers of Payment Card Incident

June 27, 2016

California residents please click here

Hard Rock Hotel & Casino Las Vegas values the relationship we have with our customers, which is why we are notifying you of an incident that may involve your payment card.

After receiving reports of fraudulent activity associated with payment cards used at the Hard Rock Hotel & Casino Las Vegas, the resort began an investigation of its payment card network and engaged a leading cyber-security firm to assist. On May 13, 2016, the investigation identified signs of unauthorized access to the resort's payment card environment. Further investigation revealed the presence of card scraping malware that was designed to target payment card data as the data was routed through the resort's payment card system. In some instances the program identified payment card data that included cardholder name, card number, expiration date, and internal verification code. In other instances the program only found payment card data that did not include cardholder name. No other customer information was involved. It is possible that cards used at certain restaurant and retail outlets at the Hard Rock Hotel & Casino Las Vegas between October 27, 2015 and March 21, 2016, could have been affected.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. 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.

We have notified law enforcement officials and are supporting their investigation. We are also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards. We also continue to work with the cyber security firm to further strengthen the security of our systems to help prevent this from happening in the future.

We regret any inconvenience this may have caused. If you have questions, please call 888-221-7168 from 9 a.m. to 9 p.m. EST, Monday to Friday.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you 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 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
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. 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 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 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 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 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 19022-2000, 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.

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.

FOR IMMEDIATE RELEASE

Hard Rock Hotel & Casino Las Vegas Notifies Customers of Payment Card Incident

Las Vegas, NV – June 27, 2016 – Hard Rock Hotel & Casino Las Vegas values the relationship it has with its customers. The resort is providing notification of an incident that may involve customer payment card data.

After receiving reports of fraudulent activity associated with payment cards used at the Hard Rock Hotel & Casino Las Vegas, the resort began an investigation of its payment card network and engaged a leading cyber-security firm to assist. On May 13, 2016, the investigation identified signs of unauthorized access to the resort's payment card environment. Further investigation revealed the presence of card scraping malware that was designed to target payment card data as the data was routed through the resort's payment card system. In some instances the program identified payment card data that included cardholder name, card number, expiration date, and internal verification code. In other instances the program only found payment card data that did not include cardholder name. No other customer information was involved. It is possible that cards used at certain restaurant and retail outlets at the Hard Rock Hotel & Casino Las Vegas between October 27, 2015 and March 21, 2016, could have been affected.

Customers who used their payment cards at certain restaurant and retail outlets at the Hard Rock Hotel & Casino Las Vegas between October 27, 2015 and March 21, 2016, should remain vigilant to the possibility of fraud by reviewing their payment card statements for any unauthorized activity. Hard Rock Hotel & Casino Las Vegas has notified law enforcement officials and is supporting their investigation. The payment card networks have also been informed of the incident so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards. Hard Rock Hotel & Casino Las Vegas continues to work with the cyber security firm to further strengthen the security of its systems to help prevent this from happening in the future.

We regret any inconvenience this may have caused. If you have questions, please call 888-221-7168 from 9 a.m. to 9 p.m. EST, Monday to Friday.