BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

June 27, 2016

VIA OVERNIGHT MAIL

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

Our client, Hard Rock Hotel & Casino Las Vegas, understands the importance of protecting the payment card information of its customers. We are writing on behalf of our client to notify you of a security incident that may have involved the payment card information of New Hampshire residents.

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.

Hard Rock Hotel & Casino Las Vegas has taken significant steps to resolve this issue and strengthen the security of its network environment. Initial measures taken to stop the attack included resetting all enterprise passwords, blocking certain network communication attempts, and removing and cleaning devices affected by the attack. To further strengthen the security of

its systems to help prevent this from happening in the future, the resort deployed point-to-point encryption and tokenization solutions for its payment card processing system. The resort has also been supporting the investigation being conducted by law enforcement officials. The payment card networks have been notified so that they can work with the banks that issued payment cards used during the at risk time period at the resort. Last, the resort has also established a dedicated call center that potentially affected individuals can call with questions regarding the incident.

Accordingly, pursuant to N.H. Rev. Stat. Ann. §359-C:20, Hard Rock Hotel & Casino Las Vegas is providing substitute notification today to New Hampshire residents who used their payment cards at Hard Rock Hotel & Casino Las Vegas between October 27, 2015 and March 21, 2016 by posting a statement on its website and issuing a press release in substantially the same form as the enclosed document. Hard Rock Hotel & Casino Las Vegas does not collect the mailing or email address of its customers for use in processing payment card transactions and is therefore not able to mail or email individual notice to affected individuals nor identify the number of New Hampshire residents that may have been affected. Notification is being provided as quickly as possible. *See* N.H. Rev. Stat. Ann. §359-C:20.

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

Sincerely,

Craig A. Hoffman
Partner

Enclosure

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.