Notice of Potential Payment Card Security Incident (12/8/2015)

CM Ebar, LLC, the owner of the Elephant Bar restaurants ("Elephant Bar"), recently became aware of a security incident possibly affecting the payment card information of some customers who made payment card purchases at certain Elephant Bar locations in California, Colorado, Arizona, Missouri, Nevada, New Mexico, and Florida. As a precaution, we are providing this notice to make potentially affected customers aware of the incident and call their attention to steps they can take to help protect themselves. We take the security of personal information very seriously, and sincerely apologize for any inconvenience or concern this incident may cause.

On November 3, 2015, Elephant Bar was alerted to a potential security incident by its card processor. Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software on our payment processing systems at certain restaurant locations designed to capture payment card information. These locations included 20 in California: Bakersfield, Burlingame, Campbell, Citrus Heights, Concord, Cupertino, Daly City, Downey, Dublin, Emeryville, Fremont, Fresno, Hayward, La Mirada, Lakewood, Montclair, Sacramento, San Marcos, Torrance and West Covina; three in Colorado: Colorado Springs, Lakewood and Greenwood Village; two in Arizona: Chandler and Peoria, and one each in Orlando, Florida, St. Louis, Missouri, Albuquerque, New Mexico, and Henderson, Nevada. We believe the malware could have compromised payment card data – including name, payment card account number, card expiration date, and verification code – of customers who used a payment card at the affected locations. Although the timing of the incident varies by location, the forensic investigation has indicated that this incident may have impacted individuals who made payment card purchases between August 12, 2015 and December 4, 2015. Please visit www.elephantbar.com/incident for a list of the affected locations, the specific time frame for each location during which we believe payment card data could have been affected, and some other helpful resources.

We are treating this matter as a top priority, and took steps to address and contain this incident promptly after it was discovered, including engaging outside data forensic experts to assist us in investigating and remediating the situation. We have disabled the malware and have reconfigured our point-of-sale and payment card processing systems to enhance the security of these systems. In addition, we are in contact with law enforcement and will continue to cooperate with its investigation. We are also coordinating with payment card companies. While we are continuing to review and enhance our security measures, the incident has now been contained and customers can safely use payment cards at all Elephant Bar locations.

We want to make potentially affected customers aware of steps they can take to guard against fraud or identify theft. We recommend that customers review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge customers to remain vigilant and continue to monitor statements for unusual activity going forward. If they see anything they do not understand or that looks suspicious, or if they suspect that any fraudulent transactions have taken place, customers should immediately notify the issuer of the credit or debit card. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although this incident did not include Social Security numbers, addresses, or other sensitive personal information, as an additional precaution, we are providing information and resources to help customers protect their identities. This includes an "Information About Identity Theft" reference guide, available on our website at www.elephantbar.com/incident, which describes additional steps customers may take to help protect themselves, including recommendations from the Federal Trade Commission regarding identity theft protection.

For more information about this incident and ways customers can protect themselves, contact us toll-free at 866-578-5412. Again, we regret any concern this incident may cause.