Locke Lord LLP
Attorneys & Counselors

Terminus 200, 3333 Piedmont Road NE, Suite 1200
Atlanta, GA 30305
Telephone: 404-870-4600
Fax: 404-872-5547
www.lockelord.com

Vita E. Zeltser
Direct Telephone: 404-870-4666
Direct Fax: 404-806-5666
vzeltser@lockelord.com

VIA OVERNIGHT FEDEX

May 30, 2013

Attorney General Michael Delaney
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Incident

Dear Attorney General Delaney:

We are counsel to Rosewood Hotels and Resorts, L.L.C., the management company for Anasazi Hotel LLC ("Anasazi"). Enclosed please find a letter from Anasazi notifying you of a recent security incident. If you have any questions regarding this incident, please do not hesitate to contact me directly.

Sincerely,

LOCKE LORD LLP

Vita E. Zeltser

CC: Kenneth Carone
Susan Aldridge

Enclosure

ROSEWOOD
INN OF THE ANASAZI®
SANTA FE

May 30, 2013

Attorney General Michael Delaney
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Incident

Dear Attorney General Delaney:

We are a hotel in New Mexico and are writing to report a data security incident that may have affected the credit card information of at least approximately 10 residents of New Hampshire.

Sometime around March 21, 2013, we were notified by the credit card processing vendor that Anasazi Hotel LLC ("Anasazi") was identified as the "common point of purchase" for a number of credit cards involved in fraudulent transactions with other merchants. The notice of common point of purchase was simply to alert Anasazi that it, perhaps with other merchants, was a merchant common to subsequent suspected fraudulent uses of payment cards used at our facility.

In response to the notice, we quickly locked down our computer network and all computer systems and engaged forensic investigators. The forensic investigation commenced immediately after we received notice of the security incident, and recently concluded. During the course of the investigation, forensic experts analyzed all aspects of our data systems to determine whether credit card information was in fact accessed without authorization. The forensic experts uncovered evidence that Anasazi was the target of cyber-attackers seeking to access parts of our internal network and data systems. During the course of the forensic examination, we learned that the cyber-attacks may have begun as early as June 18, 2012, when the attackers hacked into our system and installed malware apparently designed to perform certain functions, including eventually transmitting credit card data outside the secure network. While the forensic experts found no actual evidence that credit card information was in fact transmitted to the attackers, the forensic experts have concluded that the malware discovered on the Anasazi systems is consistent with that typically used to gather and transmit sensitive credit card data. Out of an abundance of caution, we are providing this notice to you, and plan to alert the known New Hampshire residents of the incident as expeditiously as we can, even in the absence of hard evidence that credit card data of New Hampshire residents was in fact taken by the attackers.

The portion of our computer system where the malware appears to have been installed contained names and credit card information of certain patrons of Anasazi. We do not collect Social Security Numbers or dates of birth of our hotel patrons; thus, no Social Security Numbers or dates of birth were compromised.

As of the date of this letter, our systems have been restored and are fully functional and operating with heightened system security, including restructured password protections, enhanced security software, and advanced firewall safeguards. Our efforts to enhance our security are ongoing and countermeasures will soon include real-time monitoring by a leading worldwide security services provider.

113 WASHINGTON AVENUE SANTA FE, NEW MEXICO 87501
TELEPHONE 505.988.3030 FACSIMILE 505.988.3277

We have reported these cyber-attacks to the U.S. Secret Service and will work with law enforcement authorities to identify and pursue the perpetrators involved for any and all laws that may have been broken. The law enforcement authorities did not advise us to delay any notifications in connection with this incident.

We have received assurance from our payment processing vendor that all applicable affected cardholders will be notified by either the credit card payment brand company or the credit card's issuing bank, as applicable, that there was a suspected security incident involving their credit card, and a new card number would be issued, as needed. It is likely that some of the affected credit cards have already been reissued with new numbers.

In addition to the credit card payment brand or issuing bank notifications, we are also planning to send out our own consumer notice letters to those affected individuals for whom we can locate addresses, and are using all reasonable efforts to assemble those addresses. As a merchant accepting credit cards, we do not collect addresses for persons paying with a card at our facility, which includes a hotel and a restaurant, but we do have addresses for most hotel guests that had room reservations during the timeframe of the cyber-attacks. We do not have addresses for the persons who used their credit cards at our restaurant. We have attempted to obtain addresses for cardholders that used their cards at our facility during the timeframe of the cyber-attacks from the card payment brands, via the credit card processing company, and have been advised that American Express (but none of the other card brands) will assist us in sending out our notice letters directly to the affected cardholders. Thus, all American Express cardholders, which are approximately 60% of cardholders affected by this incident, will receive our consumer notice letter. With respect to the remaining approximately 40% of affected cardholders – those that paid at our facility during the timeframe of the cyber-attacks with a VISA, MasterCard or Discover card – we will be able to send notice letters only to the addresses provided to us for purposes of making room reservations. These notices will advise the recipients that the card or cards used at our hotel during their stay may have been compromised.

Our notices to affected individuals will include a summary of the incident and our response, and inform individuals what they can and should do to protect themselves against identity theft. The notices will offer one year of free identity protection assistance with AllClear ID (formerly known as Debix, Inc.), a leading provider of such services. The identity protection assistance services will include investigators working to recover financial losses, restore credit, and make sure identity is returned to proper condition, and credit monitoring and a $1 million identity theft insurance policy services, including fraud resolution services.

We do not yet have an expected mail date for those notices. It will take more time to assemble the addresses and arrange for the mass-mailing, and for the staffing of a call bank to field questions from the recipients of the notices. At this time, our best estimate is that the total number of individuals potentially affected is less than 9,000, of which there are approximately 10 New Hampshire addresses that had reservations on record during the timeframe of the cyber-attacks.

If you or members of your staff have questions regarding the details of this incident, please contact the undersigned.

Respectfully,

Kenneth Carone, Controller
kenny.carone@rosewoodhotels.com