ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

[redacted]

[redacted]

December 19, 2014

BY FEDERAL EXPRESS

Office of the New Hampshire
Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Exposure of Personal Information*

To Whom It May Concern:

My firm represents Presidian Hotels & Resorts ("Presidian"), the manager of the Visalia Marriott at the Convention Center in Visalia, California (the "hotel"). Presidian is an independent, separate and distinct entity from Marriott International, Inc. and its affiliates. Pursuant to the provisions of N.H. Rev. Stat. Ann. §§359-C:19 et seq., I write to inform you of an incident involving the suspected unauthorized access of credit and debit card information of certain hotel guests.

The hotel believes that malware infected the point-of-sale (POS) system used for taking payment via credit or debit card in the food and beverage outlets within the hotel. The period of exposure was from July 26, 2014–September 2, 2014. The unlawfully accessed data may have included names printed on the credit or debit cards, credit or debit card numbers, the security code and card expiration dates. Guests at the hotel who did not use their credit or debit card at the hotel's food and beverage outlets, and guests who charged food or beverage purchases to their room account at these outlets, were not affected.

Presidian knows the scope of the personal information involved in this incident and has ascertained the number of possible card accounts at issue, but has been unable to obtain contact information for all of the affected individuals. Based upon the information available, Presidian knows of one potentially affected individual who resides in the State of New Hampshire.

Upon learning of the suspected data security incident, Presidian immediately deactivated the POS system, commenced an investigation, and initiated a third-party forensic review. Presidian

also reported the incident to the U.S. Secret Service. The credit card companies and issuing banks have also been advised of the incident.

Enclosed is a copy of a form of notification letter which will be sent to the single known potentially affected New Hampshire resident as well as other known affected persons who reside in other jurisdictions. The notifications will be sent via U.S. mail during the period of December 19-24, 2014. Contemporaneously with the mailing of notifications, Presidian will post a form of this notification on its website, and that posting will remain for at least 90 days from the date of posting.

If you have any further questions about the incident, do not hesitate to contact me.

Very truly yours,

Sandy B. Garfinkel

Enclosure

PRESIDIAN
HOTELS & RESORTS
Better Hospitality

9000 Tesoro Drive, Suite 300
San Antonio, TX 78217

December 19, 2014

Sample A. Sample
123 Anywhere St
Anytown, US 12345-6789

Important Credit Card Security Notification.
Please read this entire letter.

Data Security Incident at the Visalia Marriott at the Convention Center

Dear Sample A. Sample,

We are writing to inform you of an incident at the Visalia Marriott at the Convention Center in Visalia, California (the "hotel") that may affect you. This hotel is managed by Presidian Hotels & Resorts (Presidian), a hotel management company. Presidian is an independent, separate and distinct entity from Marriott International, Inc. We believe that there may have been unauthorized access to credit and debit card data for cards used at food and beverage outlets at the hotel during the period of July 26, 2014 – September 2, 2014. Because you were a guest of the hotel during this period and used a credit or debit card at one of the food and beverage outlets, we are writing to notify you of this situation. We suspect there was unauthorized access because we found malicious software (also known as malware) present on the point-of-sale (POS) system used for taking payment via credit or debit card in the food and beverage outlets at the hotel. The unlawfully accessed data may have included names printed on the credit or debit cards, credit or debit card numbers, security codes and card expiration dates. Please note that guests at the hotel who did not use their credit or debit cards at these outlets, and guests who charged food or beverage purchases to their room account at these outlets, are not at risk.

Upon learning of the suspected data security incident, we immediately deactivated the POS system, commenced an investigation, and initiated a third-party forensic review. We also informed appropriate federal law enforcement officials of the incident[1]. We continue to work with investigators and the credit card companies and are actively taking steps to prevent a reoccurrence. We have also posted additional information about this incident on our website at **www.presidian.com**.

[1] This notification was not delayed as a result of a law enforcement investigation.

While the financial institutions that have issued the credit or debit cards that are potentially affected by this incident are already aware of this situation and are increasing their fraud monitoring or have reissued the cards, if you suspect unauthorized activity you should report it to the issuer of the credit or debit card immediately. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you have zero liability for any unauthorized charges if you report them in a timely manner.

You are urged to be vigilant for signs of fraud or identity theft by reviewing your account statements and obtaining and reviewing your free credit report concerning your credit activity. There are instructions for obtaining your free credit report in the attached pages. If you suspect that fraud or identity theft has occurred, you should report it to your local law enforcement agency, to your state's attorney general's office and/or to the U.S. Federal Trade Commission ("FTC") (contact information for the FTC is provided in the attached pages).

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: March 31, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: xxxxxxxxx**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **PC90477.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance**[2]**:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

[2] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-371-7902. Additional resources regarding avoiding and understanding identity theft can be found in the section of this letter titled "Additional Resources, Credit Alerts and Freezes."

Please note when these types of incidents occur, some criminals seek to fraudulently obtain the personal information of affected individuals by claiming to be the business that experienced the incident. We advise you NOT to respond to any requests from entities requesting your sensitive personal information in relation to this incident. The hotel, Presidian, Experian or anyone legitimately contacting you on their behalf will NOT ask you for other sensitive personal information with regard to this incident. We will only ask for the most limited amount of information necessary to provide the identity protection services. If you receive any suspicious looking written or electronic requests purporting to be from the hotel, Presidian, Experian or anyone please call us at 1-888-490-2440.

Note: If you decide to enroll in Experian's ProtectMyID membership you will be required to provide your personal information including your Social Security number to verify your identity. You will also receive messages from Experian regarding your membership and credit alerts.

We deeply regret and apologize that this incident has occurred and reaffirm our commitment to protect the personal information you entrust to us. If you have questions regarding this situation and the actions you can take to protect yourself, or the complimentary identity theft protection services, please call us at 1-888-490-2440.

Sincerely,

Charles Leddy
Chief Executive Officer

ADDITIONAL RESOURCES, CREDIT ALERTS AND FREEZES

Information about Identity Theft

Federal Trade Commission
The Federal Trade Commission provides helpful information about how to avoid identity theft.

- Visit: http://www.ftc.gov/idtheft
- Call (toll-free): 1-877-ID-THEFT (1-877-438-4338)
- Write: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.

Free Annual Credit Reports

You may obtain a free copy of your credit report once every 12 months.

- Visit: http://www.annualcreditreport.com
- Call (toll-free): 1-877-322-8228
- Write: Complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the form at http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf).

You also may purchase a copy of your credit report by contacting one of the three national credit reporting companies.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P. O. Box 740241	P. O. Box 9554	2 Baldwin Place
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19022

Fraud Alerts: "Initial Alert" and "Extended Alert"

You can place two types of fraud alerts on your credit report to put your creditors on notice that you may be a victim of fraud: an "Initial Alert" and an "Extended Alert." An Initial Alert stays on your credit report for 90 days. You may ask that an Initial Alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An Extended Alert stays on your credit report for seven years. To obtain the Extended Alert, you must provide proof to the credit reporting company (usually in the form of a police report) that you actually have been a victim of identity theft. You have the right to obtain a police report regarding the data security incident. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three credit reporting companies provided above.

A potential drawback to activating a fraud alert would occur when you attempt to open a new account. You would need to be available at either your work phone number or home phone number in order to approve opening the new credit account. If you are not available at either of those numbers, the creditor may not open the account. In addition, it may take longer to obtain credit and in some cases merchants may be hesitant to open a new account.

Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is not required by law to contact you if you have a fraud alert in place. Fraud alerts can legally be ignored by creditors. If you suspect that you are or have already been a victim of identity theft, fraud alerts are only a small part of protecting your credit. You also need to pay close attention to your credit report to make sure that the only credit inquiries or new credit accounts in your file are yours.

You may contact all of the three major credit reporting agencies using the information below that they have published. Credit agencies will need to verify your identity which will require providing your Social Security number and other similar information.

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
https://fraud.transunion.com
1-800-680-7289

Equifax
P. O. Box 740241
Atlanta, GA 30374-0241
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
1-888-766-0008

Experian
P. O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
1-888-397-3742

Placing a fraud alert does not damage your credit or credit score. Additional information may be obtained from www.annualcreditreport.com.

Credit or Security Freeze on Credit File

In some U.S. states, you have the right to put a credit freeze (also known as a security freeze) on your credit file. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. If permitted in your State, using a security freeze may interfere with, or delay your ability to obtain credit.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit report, contact the credit reporting agencies using the information below, and be prepared to provide the following (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well):

(1) full name, with middle initial and any suffixes;
(2) Social Security number;
(3) date of birth;
(4) current address and any previous addresses for the past two years; and
(5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of between $5.00 and $20.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. The addresses of consumer reporting agencies to which requests for a security freeze may be sent are:

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
https://freeze.transunion.com

Equifax
Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian
P. O. Box 9532
Allen, TX 75013
https://www.experian.com/freeze/center.html

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 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);
- the PIN or password provided to you when you placed the security freeze; and
- the identities 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.