



**WYNDHAM  
HOTELS AND  
RESORTS**

August 21, 2009

The Honorable Martha Coakley  
Attorney General, State of Massachusetts  
One Ashburton Place  
Boston, MA 02108

Dear Attorney General Coakley:

We write to provide you an update to the security incident about which we notified you in September, 2008, involving information held by franchised and managed properties of Wyndham Hotels and Resorts, LLC ("WHR") ("2008 Data Incident"). As previously requested, we seek confidential treatment for this letter and all future written and verbal correspondence related to this matter. We are coordinating this notice on behalf of WHR and its franchised and managed properties.

During the on-going remediation process of the 2008 Data Incident, in mid-May, 2009, WHR received notice of potential fraudulent use of credit cards in which one of its properties was identified as the Common Point of Purchase for a transaction which occurred in mid-March. WHR promptly retained a Qualified Investigative Response Assessor to conduct a thorough investigation, which is virtually complete at this time. To date, our investigation of this new incident has confirmed that a sophisticated hacker used a different method of ingress to penetrate the computer systems of the WHR Data Center and thereafter was able to view and acquire credit card information via a malicious memory resident malware. We have reason to believe that the hacker was able to access both track one and track two data on credit cards. Our investigation discloses that approximately 1,146 residents in the state of Massachusetts were impacted by this second incident.

In addition to ensuring that the hack was immediately terminated and disabled, WHR promptly notified the Secret Service and each of the payment card networks about the incident. We also have notified the affected managed and franchised hotels to ensure that their systems are properly investigated and secured, and to determine how, if at all, those systems were involved in the incident.

Because postal addresses were not found in the compromised files or in the file created by the hacker, it has taken several weeks to confirm the window of vulnerability and determine the names and addresses of the consumers potentially impacted. Having now completed that process, we will notify the consumers who engaged in transactions during that period of the potential acquisition of their card data. In addition, we will provide one year of credit card monitoring services, as well as such other information as

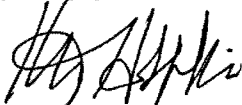
The Honorable Martha Coakley  
Attorney General, State of Massachusetts  
August 21, 2009  
Page 2 of 2

is appropriate to help the consumers protect their interests. We attach a copy of the notice to be sent to consumers for your records.

Pursuant to Massachusetts law, we are also providing a similar notification to the Director of Consumer Affairs and Business Regulation.

If you have any further questions about either incident, do not hesitate to contact me at (973) 753-6475, or [Kirsten.Hotchkiss@WyndhamWorldwide.com](mailto:Kirsten.Hotchkiss@WyndhamWorldwide.com)

Very truly yours,



KIRSTEN HOTCHKISS  
Senior Vice President – Legal and Assistant Secretary  
Wyndham Hotels and Resorts, LLC

Enclosure



August 2009

Endorsement Line  
Joe Sample  
123 Anytown  
Suite 456  
Your Town, USA 99999-9999

11  
00001

Promotion Code:  
XXXXXXXXXXXXXXXXXX



Dear Joe Sample:

We are writing to inform you of a data security incident involving your personal information. Wyndham Hotels and Resorts ("Wyndham") is coordinating the response to this incident on behalf of Wyndham's managed and franchised hotels. The incident discussed in this letter occurred only at certain Wyndham branded hotels.

As a result of unauthorized access to Wyndham systems, Wyndham has determined that your credit or debit card number, expiration date and possibly your name were compromised. Wyndham has taken numerous steps to protect your information since the discovery of this incident. In addition to terminating the unauthorized access, we revalidated our information security infrastructure to confirm that we maintain industry standard protections for customer data. In addition, we promptly notified law enforcement and each of the major payment card networks (American Express, Visa, MasterCard, and Discover). **We also provided each of the payment card companies with the actual credit and debit card numbers that had been involved in the incident so that the payment card companies could take such action as they deemed appropriate.** We also notified the affected hotels so that they could take the appropriate action to ensure that their systems are properly investigated and secured.

Even though we have taken this action to protect your information, we nevertheless recommend that you remain vigilant with respect to reviewing your account statements and credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities.

The Federal Trade Commission also provides helpful information about how to avoid identity theft. Please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (1-877-438-4338).

You may obtain a free copy of your credit report from each of the 3 major credit reporting companies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to: Annual Credit Report Request Service, P. O. Box 105281, Atlanta, GA 30348-5281. You can print a copy of the request form from <http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm>. You also may purchase a copy of your credit report by contacting one of the three national credit reporting companies shown here:

Equifax (800) 685-1111 <a href="http://www.equifax.com">www.equifax.com</a> P. O. Box 740241 Atlanta, GA 30374-0241	Experian (888) 397-3742 <a href="http://www.experian.com">www.experian.com</a> P. O. Box 9532 Allen, TX 75013	TransUnion (800) 916-8800 <a href="http://www.transunion.com">www.transunion.com</a> P. O. Box 6790 Fullerton, CA 92834-6790
---	---	--

\* \* \* \* \*

Each of these companies offers services involving credit monitoring, and, depending upon state law, identity theft insurance. The prices of these services range from a low of \$6.95 per month for weekly alerts to a high of \$39.95 per month for daily alerts. However, to assist you in protecting your credit, Wyndham is offering to you, at no cost, for one year, Equifax Credit Watch™ 3-in-1 Alerts product. **To take advantage of this product offer, you must enroll no later than November 30, 2009.** This product provides:

- o Comprehensive credit file monitoring of your Equifax, Experian, and TransUnion credit reports with daily notification of key changes to your credit files from any of the three agencies
- o Up to \$1 million in identity theft protection with \$0 deductible, at no cost to you.
- o 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and to you assist in initiating an investigation of inaccurate information

---

\* Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for complete details of coverage and exclusions.

must separately place a credit freeze on your credit file at each credit reporting company. ***Please note that placing a credit freeze on your credit file at one or more of the credit reporting companies will prevent you from participating in the Equifax Credit Watch™ 3-in-1 Alerts product from Equifax.***

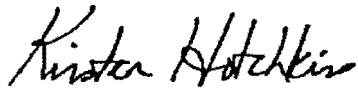
\* \* \* \* \*

Please note that in the aftermath of security breaches, some criminals seek to fraudulently obtain personal information of affected individuals by claiming to be the business experiencing the breach. We wish to advise you that you should **NOT** respond to any requests from entities requesting your sensitive personal information in relation to this breach. Wyndham will **NOT** ask you for your Social Security Number or other sensitive personal information with regard to this incident, other than as may be necessary to respond to questions from you about how the incident may have impacted you. If you receive any written request or electronic request via e-mail purporting to be from Wyndham and it looks suspicious, please call us for assistance at the number provided below.

In addition, for a limited time, we are offering a Preferred Customer Rate discount program for our customers who may have been impacted by this incident. You will receive a 20% discount on the room rate for any hotel stays with a Wyndham brand hotel when you make your reservations on or before December 15, 2009. To take advantage of this offer via telephone, you may call 1-800-WYNDHAM and ask for the PREFERRED GUEST RATE or ask for the rate for Corporate ID 43783670. To take advantage of the discount online, please visit [www.wyndham.com](http://www.wyndham.com), and under "Find Locations" select the property at which you want to stay and click "View This Hotel." At that point, you should enter your travel details, click on Search using Corporate, Promo and Group codes, enter Corporate ID 43783670 and then search for rates.

Wyndham deeply regrets that this incident has occurred. Therefore, we have established the following toll-free number to handle your inquiries about the actions you can take to protect yourself. Should you have any questions, please call 1-888-355-2327, between 7AM and 10PM Central Time, 7 days a week.

Sincerely,



Kirsten Hotchkiss  
Senior Vice President  
Wyndham Hotels and Resorts, LLC

## How to Enroll

To sign up online for online delivery go to [www.myservices.equifax.com/3in1alerts](http://www.myservices.equifax.com/3in1alerts). For live agent enrollment assistance from Equifax, please call 1-866-252-4576. **All consumer information, identity verification, and payment information you enter on the following pages will be kept in a secured environment.**

1. **Consumer Information:** Complete the form with your contact information (name, address and e-mail address) and click "Continue" button.
2. **Identity Verification:** Complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.
3. **Payment Information:** The promotion code provided at the top of the first page of this letter constitutes payment for the service. During the "Check Out" process, enter the promotion code in the "Enter Promotion Code" box. After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page.
4. **Order Confirmation:** – Click "View My Product" to access the product features.

\* \* \* \* \*

In addition, you may consider placing a fraud alert, which will add a statement to your credit file. This statement alerts creditors to possible fraudulent activity within your file and requests that the creditor contact you prior to establishing any accounts in your name. There are two types of fraud alerts that you can place on your credit file 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 file for 90 days. You may ask that an Initial Alert be placed on your credit file if you suspect you have been, or are about to be, a victim of identity theft. An Extended Alert stays on your credit file for seven years. In order 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 can place a fraud alert on your credit file by calling the toll-free number of any of the three credit reporting services provided above. Additional information may be obtained from [www.annualcreditreport.com](http://www.annualcreditreport.com).

In some U.S. states, you have the right to put a credit freeze (also known as a security freeze) on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit file without your consent. **Therefore, using a credit freeze may interfere with or delay your ability to obtain credit.** Since the instructions for how to establish a credit freeze differ from state to state, please contact one of the three major reporting companies at the numbers above to find out more information. There may be fees for placing, lifting, and/or removing a credit freeze, which generally range from \$5-20 per action. Unlike a fraud alert, you