

**DRAFT 5/7/12**

[LOGO]

\_\_\_\_\_, 2012

[Consumer Name]  
[Consumer Street Address]  
[Consumer City, State, Zip]

***Important Information Security and Protection Notification.  
Please read this entire letter.***

Re: **Theft of Personal Information**  
Crowne Plaza Columbus, Ohio

Dear \_\_\_\_\_:

We are writing to inform you of a data security incident at the Crowne Plaza, Columbus, Ohio (the "Hotel"). The data security incident includes credit card information, meaning, among other things, the name, address, credit card number and expiration date of certain credit cards used at the Hotel.

The theft of personal information was first identified in the beginning of April of this year, when InterContinental Hotels Group notified the Hotel that malware was present on the front desk computers of the Hotel. This malware had been unknowingly downloaded by an employee when updating the Hotel's software. The malware was active for a period of approximately ten (10) days beginning in mid-March of this year. While the malware was active, it is possible that your credit card information, including your name, address, credit card number and expiration date may have been exposed. The Hotel has reported this data security incident to the appropriate law enforcement authorities and has notified each of the major payment card networks (American Express, Visa, Mastercard, and Discover) of the incident.

Furthermore, the Hotel immediately removed the front desk computers with malware and installed new computers. In addition, InterContinental Hotels Group immediately blocked malware communications generated from the computers at the Hotel to prevent further transmission of the malware or any further transmission of personal data.

We are providing this notice to alert you to the possibility that the compromised information could be used to commit identity theft. The fact that we do not know the location of this data that includes some of your own personal information puts you personally at risk for future identity theft or other abuse or unauthorized use of the information.

For your information, the Hotel has reviewed and modified its practices in storing and safeguarding Hotel guest's credit card information to minimize the risk of such an event

**DRAFT 5/7/12**

ever occurring in the future. In addition, the Hotel has provided training to Hotel employees to recognize and be aware of malware risks in the future.

We recommend that you remain vigilant and review your account statements and credit reports regularly. 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 local law enforcement authorities.

**To assist you in identifying possible identity theft, you will be provided with monitoring, at no cost to you, through Debix Identity Protection.** Debix offers credit monitoring that delivers credit alerts to you by phone. Debix Identity Protection also includes \$1,000,000 identity theft insurance coverage and Debix Fraud Resolution Services. The Debix Identity Protection service will be valid for 1 year from the date you register. Enclosed you will find a page that generally describes Debix’s service and how to register by telephone (866-979-2595), mail or on Debix’s website ([www.debix.com/safe](http://www.debix.com/safe)). You must register with Debix to receive the identity protection service. Also enclosed with this letter is a form to register for the service by mail if you choose to register via mail.

The Federal Trade Commission also provides helpful information about how to avoid identity theft. Please visit <http://www.ftc.gov/idtheft>, call 1-877-ID-THEFT (877-438-4338) or write to the Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, H-130, Washington, DC 20580.

You may obtain a free copy of your credit report once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 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 at <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.

Equifax (800) 525-6285 <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 Fraud Victim Assistance Division (800) 680-7289 <a href="http://www.transunion.com">www.transunion.com</a> P. O. Box 6790 Fullerton, CA 92834-6790
---	---	--

In addition, there are two types of fraud alerts that you can place 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. In order to obtain the Extended Alert, you must provide proof to the credit

## ***DRAFT 5/7/12***

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 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. 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.

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, send a request by mail to a consumer reporting agency at the address below that includes 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. Here are the addresses of consumer reporting agencies to which requests for a security freeze may be sent:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

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.

## ***DRAFT 5/7/12***

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.

Please note that after an information loss or security breach, 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 incident. No one from the Hotel nor anyone legitimately contacting you on its behalf will 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 the Hotel or a company affiliated with the Hotel, and the request looks suspicious, please call us for assistance at the number provided below. **Note:** If you decide to enroll in the credit monitoring service you will be required to provide your Social Security number to verify your identity.

Again, we have no knowledge that your own personal information has been further accessed, used or disclosed; however, we wish to ensure that you are forewarned and able to identify any suspicious account activity.

We deeply regret that this incident has occurred and reaffirm our commitment to protect the personal information you entrust to us.

Erica Hageman  
Senior Corporate Counsel  
703 387-3100

*Enclosures*