

TO: CPB: Security Breach Notification

FAX NO.: 518-474-2474

FROM: Cathy Bump
Hotels.com

TEL.: 425-679-7251

DATE: June 1, 2006

NO. PAGES: 1 + 4

*Dwight -
Pls make
file "Hotels.Com"*

**Reporting Form
 For Business, Individual or NY State Entity reporting a
 "Breach of the Security of the System"
 Pursuant to the Information Security Breach
 and Notification Act (General Business Law §889-aa;
 State Technology Law §208)**

Name of Business, Individual or State Entity: Hotels.com
 Date of Discovery of Breach: May 3, 2006
 Estimated Number of Affected Individuals: 16,478
 Date of Notification to Affected Individuals: May 26 - June 2, 2006
 Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

Ernst + Young, as external auditor of Hotels.com, had names, addresses + credit card data of Hotels customers on an employee's laptop. Laptop was stolen from a locked car. No evidence to date of misuse of the data.

Name of Business or Individual Contact Person: Cathy Bump
 Title: Senior Privacy Compliance Counsel
 Telephone number: 425-679-3610
 Email: cbump@expedia.com

Dated: May 30, 2006
 Submitted by: Cathy Bump
 Title: Senior Privacy Compliance Counsel
 Address: 3150 139th Ave. SE, Bellevue, WA 98005
 Email: cbump@expedia.com
 Telephone: 425/679-3610 Fax: 425/679-7251

Hotels.com
P.O. Box 27550
Santa Ana, CA 92799

May 26, 2006

[Name]
[Address 1]
[Address 2]
[City, State, Zip]

Important Information Regarding Your Card Ending [XXXX] [(Insert Card Type)]

Dear [Name]:

Recently, Hotels.com was informed by its outside auditor, Ernst & Young, that one of Ernst & Young's employees had his laptop computer stolen. Unfortunately, the computer contained certain information about customer transactions with Hotels.com, and other sites through which we provide booking services directly to customers, from 2002 through 2004. This information may have included your name, address and some credit or debit card information you provided at that time. We sincerely regret that this incident occurred and we are taking it very seriously.

The data in question was provided to Ernst & Young as part of an audit required by law. Since first learning of this incident from Ernst & Young, we have been working to determine what information was on the laptop computer, consulting with law enforcement officials regarding their investigation of the crime, working with the credit card companies to mitigate the risk of credit card fraud, and identifying and notifying potentially impacted Hotels.com customers. The computer was password protected and, after consultation with law enforcement officials, we have no reason to believe any fraud or misuse of the data has resulted from this theft. Nonetheless, we wanted to notify you promptly of this incident.

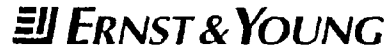
We have attached a memorandum from Ernst & Young, which explains what occurred, steps you can take to protect yourself, and services that are being made available to you at our request, including an option to enroll in a credit monitoring program, at no cost to you. It is important to know that U.S. consumers are generally protected in case of fraudulent purchases made on their credit or debit card. Nonetheless, we strongly encourage you to review the attached memorandum and to make use of the guidance and services offered by Ernst & Young to assist you in protecting against possible fraudulent use of your card information. Please do not hesitate to contact the special call center that has been established to answer any questions you may have — toll-free (866) 387-2242, or (201) 872-0169 for customers outside the United States or Canada.

Protecting the privacy and security of our customer information is extremely important to us. In that regard, we have received assurances that Ernst & Young is taking additional steps to protect the confidentiality of its data, including encrypting the sensitive information we provide to them as part of the audit process.

Over 1000 employees at Hotels.com work hard every day to earn your business and provide you with great travel deals. Our mission is to help you find the best lodging, rental car or airline ticket for your travels because we love helping our customers. We are deeply sorry that this event has occurred and regret any inconvenience it may cause you. We promise to work even harder to be your travel partner of choice and hope that you will continue to allow us to earn your trust and your business.

Sincerely,

/s/ SEAN KELL
Sean Kell
General Manager
Hotels.com

**MEMORANDUM**

TO: Hotels.com Customers

FROM: Ernst & Young

DATE: May 2006

RE: *Important Information Regarding Hotels.com Customer Information*

For the past several years, Ernst & Young has been the provider of auditing services for Hotels.com. We are writing to inform you about the theft of an Ernst & Young laptop computer that contained information on some Hotels.com customer transactions.

The laptop in question was in a backpack that was stolen from the locked vehicle of an Ernst & Young employee. The crime was promptly reported to law enforcement agencies, and there is no indication that the thief was specifically targeting the laptop or any information contained on it. We deeply regret this incident has occurred and want to apologize to you and Hotels.com for any inconvenience or concern this may cause.

Following the theft, we commenced an internal investigation of this matter and determined that the stolen computer contained certain personal information regarding some Hotels.com customer transactions primarily from the year 2004. There were also a small number of transactions from 2003 and 2002. We believe the transactions may have involved the payment card you used with Hotels.com or another website through which Hotels.com provided booking services directly to customers. Specifically, the information on the laptop may have included your name, address and some credit or debit card information you provided.

The laptop required a password to use it. The relevant file was stored in a subdirectory several levels below the computer's main directory, and the file's name gave no indication of its contents. To date, we have received no information from law enforcement officials that any of the data stored on the computer has been accessed by an unauthorized person or used improperly.

While we have no reason to believe the files have been compromised, it is still prudent to take precautions. We therefore strongly recommend that you monitor your credit card statements, beginning with those received in March, for any unauthorized charges and, if you notice any suspicious activity, contact your card issuing company immediately.

In addition, to assist you in this process and further protect you, we have worked with Hotels.com to provide the following:

- We have set up a call center with a special toll-free number — (866) 387-2242, or, if you are outside the United States, +1 (201) 872-0169 — to assist you with questions or concerns you may have related to this incident. This call center will be staffed from 9:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, from now until September 29, 2006. Callers may leave a message after hours and they will receive a call back on the next business day. *Please note that, to protect your privacy, neither Ernst & Young nor Hotels.com will email or call you to ask you to provide any additional personal information.*
- We have arranged for you, at your option, to enroll in credit monitoring, at no cost to you, for one year. Once you enroll, you will receive communications detailing any key changes to your credit reports from all three credit bureaus. If there is no activity, you will be updated on a monthly basis. To enroll in this service, please visit <http://partner.consumerinfo.com/ey> and enter the code provided below. You will be instructed on how to initiate your online membership. If you do not have internet access, please contact the call center number above for additional assistance.

Website for enrollment: <http://partner.consumerinfo.com/ey>

Your Promotional Code: [Insert individual promotional code]

- We have contacted the three major U.S. credit bureaus to inform them of this incident. Upon receiving a request from you, the agencies will place a "fraud alert" on your file, which alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit. There is no charge for you to place a fraud alert on your credit file. Should you wish to place a fraud alert, contact any one of the following bureaus:

<u>Agency</u>	<u>Toll-Free</u>	<u>International Toll</u>	<u>Website</u>
Experian.....	888-397-3742	N/A	www.experian.com
Equifax.....	800-525-6285	678-795-7831	www.equifax.com
TransUnion.....	800-680-7289	N/A	www.transunion.com

You are also entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228. For additional information on how to further protect yourself against credit card fraud, you may wish to visit the web site of the U.S. Federal Trade Commission at www.consumer.gov/idtheft/.

Please know that protecting our clients and the privacy and sensitive information of their customers is something we take very seriously at Ernst & Young. We sincerely apologize for this unfortunate incident and have instituted enhanced security procedures to encrypt all of our laptop computers to provide additional protection for sensitive information, and have taken other measures designed to protect against this type of incident happening again.