

EXHIBIT 1



CIVIL INVESTIGATIVE DEMAND

1. TO

Wyndham Worldwide Corporation
c/o Scott G. McLester, General Counsel
22 Sylvan Way
Parsippany, NJ 07054

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

You are required to appear and testify.

LOCATION OF HEARING	YOUR APPEARANCE WILL BE BEFORE
	DATE AND TIME OF HEARING OR DEPOSITION

- You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.
- You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

January 9, 2012

3. SUBJECT OF INVESTIGATION

See attached resolution

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN

Kristin Krause Cohen
601 New Jersey Ave., NW NJ-8100
Washington, DC 20001
Deputy Records Custodian: Lisa Schifferle

5. COMMISSION COUNSEL

Kristin Krause Cohen/Lisa Schifferle
601 New Jersey Ave., NW NJ-8100
Washington, DC 20001
(202) 326-2276/(202) 326-3377

DATE ISSUED

12/8/11

COMMISSIONER'S SIGNATURE

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

A copy of the Commission's Rules of Practice is available online at <http://bit.ly/FTCRulesofPractice>. Paper copies are available upon request.

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature _____

Title _____

Sworn to before me this day

Notary Public

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

**RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC
INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY
AND/OR DATA SECURITY**

File No. P954807

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.


Donald S. Clark
Secretary

Issued: January 3, 2008

**CIVIL INVESTIGATIVE DEMAND
SCHEDULE FOR PRODUCTION OF DOCUMENTS
AND ANSWERS TO WRITTEN INTERROGATORIES
TO WYNDHAM WORLDWIDE CORPORATION**

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

- A. **“Access Letter”** shall mean the April 8, 2010 letter to **Wyndham Hotels** from Commission attorney Lisa Schifferle, attached hereto as Exhibit A.
- B. **“Access Letter Response”** shall mean the July 19, 2010 letter response from Douglas H. Meal, on behalf of **Wyndham Hotels**, to the **Access Letter**, as well as any supplemental responses provided, including on September 8, 2010, September 14, 2010, January 1, 2011, and June 29, 2011.
- C. **“And,”** as well as **“or,”** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in the Schedule all information that otherwise might be construed to be outside the scope of the specification.
- D. **“Any”** shall be construed to include **“all,”** and **“all”** shall be construed to include the word **“any.”**
- E. **“Company”** or **“you”** or **“your”** shall mean collectively **Wyndham Worldwide, The Hotel Group, Wyndham Hotels, and Hotel Management.**
- F. **“Card Association”** shall mean Visa, MasterCard, American Express, Discover, or any organization that licenses **payment cards.**
- G. **“CID”** shall mean this Civil Investigative Demand, including the attached Resolution and this Schedule, and including the Definitions, Instructions, and Specifications.
- H. **“Compromised personal information”** shall mean **personal information** that was or may have been accessed or used without authorization.
- I. **“Data breach”** shall mean, and information shall be provided separately for, each instance involving access by unauthorized individuals of any **Wyndham entity’s** computer system.
- J. **“Document”** shall mean the complete original and any non-identical copy, regardless of origin or location, of any written, typed, printed, transcribed, taped, recorded, filmed, punched, computer stored, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice,

memorandum, note, telegram, report, record, audio and visual recordings and transcripts thereof, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book, label, file or folder label, draft, metadata and other bibliographic or historical data describing or relating to documents created, revised, or distributed on computer systems, copy that is not an identical duplicate of the original (whether different from the original because of notations on the copy or otherwise), and copy the original of which is not in the possession or custody of the **Company**. This definition includes **Electronically Stored Information**.

- K. **“Each”** shall be construed to include **“every,”** and **“every”** shall be construed to include **“each.”**
- L. **“Electronically Stored Information” (“ESI”)** shall mean the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created, electronically stored, or computer generated information, including but not limited to electronic mail, instant messaging, videoconferencing, and direct connections or other electronic correspondence (whether active or deleted), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, cell phones, Blackberry, PDA, print-outs, or other storage media, and such other codes, technical assistance, or instructions as will transform such ESI into an easily understandable and usable form.
- M. **“FTC”** or **“Commission”** shall mean the Federal Trade Commission.
- N. **“Hotel Management”** shall mean Wyndham Hotel Management, Inc., its wholly or partially owned subsidiaries, unincorporated divisions, business units, joint ventures, partnerships, operations under assumed names, and predecessor companies, and all directors, officers, managers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
- O. **“Identify”** or **“identifies:”**
1. when used in reference to a natural person, means to state the person’s: (a) full name; (b) present or last known residence and telephone number and present or last known business address and telephone number; (c) last known e-mail address; (d) present or last known employer and job title; and (e) the nature (including job title) and dates of any affiliation, by employment or otherwise, with the **Company**;

2. when used in reference to a corporation or other non-natural person, means to:
(a) state that entity's name; (b) describe its nature (e.g., corporation, partnership, etc.); (c) state the address of its principal place of business; (d) identify the natural person or persons employed by such entity whose actions on behalf of the entity are responsive to the CID, and that person's last known telephone number and e-mail address; and
 3. when used in reference to facts, acts, events, occurrences, meetings, or communications, means to describe with particularity the fact, act, event, occurrence, meeting, or communication in question, including but not limited to:
(a) identifying the participants and witnesses of the fact, act, event, occurrence, meeting, or communication; (b) stating the date or dates on which the fact, act, event, occurrence, meeting, or communication took place; (c) stating the location or locations at which the fact, act, event, occurrence, meeting, or communication took place; and (d) providing a description of the substance of the fact, act, event, occurrence, meeting, or communication.
- P. **"Information Security Program"** shall mean policies, practices, and procedures to protect **personal information**.
- Q. **"Intruder"** shall mean each person or entity that accessed or used **compromised personal information**, including persons and entities within or outside the **Company**.
- R. **"Payment cards"** shall mean credit cards, debit cards, gift cards, stored-value cards, or any other cards presented by a consumer to purchase goods or services.
- S. **"Payment Card Industry Data Security Standard"** or **"PCI DSS"** shall mean the information security standard for organizations that handle **payment card** information, as established by the Payment Card Industry Security Standards Council.
- T. **"Personal information"** shall mean individually identifiable information from or about an individual consumer, including, but not limited to: (1) first and last name; (2) home or other physical address, including street name and name of city or town; (3) email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) telephone number; (5) date of birth; (6) government-issued identification number, such as a driver's license, military identification, passport, or Social Security number, or other personal identification number; (7) financial information, including but not limited to: investment account information; income tax information; insurance policy information; checking account information; and **payment card** or check-cashing card information, including card number, expiration date, security number (such as card verification value), information stored on the magnetic stripe of the

card, and personal identification number; (8) employment information, including, but not limited to, income, employment, retirement, disability, and medical records; (9) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (10) any information from or about an individual consumer that is combined with any of (1) through (9) above. For the purpose of this definition, an individual consumer shall include an “employee,” and “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under your control.

- U. **“Referring to” or “relating to”** shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.
- V. **“Service Provider”** shall mean any third party that receives, maintains, processes, or otherwise is permitted access to **personal information** in the course of providing services to any **Wyndham entity**.
- W. **“Store[d] and process[ed]”** shall mean to store, collect, maintain, process, transmit, forward, handle, or otherwise use.
- X. **“The Hotel Group”** shall mean Wyndham Hotel Group, LLC, its operations under assumed names, predecessor companies, and all directors, officers, managers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
- Y. **“Wyndham entity”** shall mean any of the following: **Wyndham Worldwide, The Hotel Group, Wyndham Hotels, or Hotel Management**.
- Z. **“Wyndham Worldwide”** shall mean Wyndham Worldwide Corporation, its parents, operations under assumed names, and predecessor companies, and all directors, officers, managers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.
- AA. **“Wyndham Hotels”** shall mean Wyndham Hotels and Resorts, LLC, its wholly or partially owned subsidiaries, unincorporated divisions, business units, joint ventures, partnerships, operations under assumed names, and predecessor companies, and all directors, officers, managers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

- BB. **“Wyndham-branded hotels”** shall mean any hotel licensed to use the Wyndham name that is operated in the United States under a management or franchise agreement with **Wyndham Hotels** or **Hotel Management**.
- CC. **“Wyndham-franchised hotels”** shall mean any hotel licensed to use the Wyndham name that is operated in the United States under a franchise agreement with **Wyndham Hotels**.
- DD. **“Wyndham-managed hotels”** shall mean any hotel licensed to use the Wyndham name that is operated in the United States under a management agreement with **Hotel Management**.

II. INSTRUCTIONS

- A. **Sharing of Information.** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11 (c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.
- B. **Meet and Confer:** You must contact **Kristin Cohen** at **(202) 326-2276** as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your response, including but not limited to a discussion of the submission of Electronically Stored Information and other electronic productions as described in these Instructions.
- C. **Applicable Time Period.** Unless otherwise directed in the specifications, the applicable time period for this request shall be from January 1, 2008, until the date of full and complete compliance with this CID.
- D. **Claims of Privilege.** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:
1. the type, specific subject matter, and date of the item;
 2. the names, addresses, positions, and organizations of all authors and recipients of the item; and
 3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

- E. **Document Retention.** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. As instructed in the Access Letter, the Company should have suspended any routine procedures for document destruction and taken other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether the Company believes such documents are protected from discovery by privilege or otherwise. See 15 U.S.C. § 50; see also 18 U.S.C. §§ 1505, 1519.
- F. **Petitions to Limit or Quash.** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).
- G. **Modification of Specifications.** If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with the Commission representatives identified at the end of these instructions. All such modifications must be agreed to in writing by Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection. 16 C.F.R. § 2.7(c).
- H. **Certification.** A responsible corporate officer shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.
- I. **Scope of Search.** This CID covers documents and information in your possession or under your actual or constructive custody or control, including, but not limited to, documents in the possession, custody, or control of your attorneys, accountants, other agents or consultants, directors, officers, and employees, whether or not such documents were received from or disseminated to any person or entity. Responsive documents include those that exist in machine-readable form, including documents stored in personal computers, portable computers, workstations, minicomputers, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of offline storage, whether on or off Company premises.

- J. **Document Production.** You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Kristin Cohen, Federal Trade Commission, 601 New Jersey Avenue, N.W., Mail Stop NJ-8100, Washington, D.C. 20001. Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS. Notice of your intended method of production shall be given by mail or telephone to one of the Commission representatives identified at the end of these Instructions at least five (5) days prior to the return date.
- K. **Document Identification.** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. If the Company has previously answered any interrogatories, your response should so indicate by identifying the date of submission and the page numbers where the information can be located. Documents should be produced in the order in which they appear in your files or as electronically stored and without being manipulated or otherwise rearranged; if documents are removed from their original folders, binders, covers, containers, or electronic source in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, container, or electronic media or file paths from which such documents came. In addition, number by page (or file, for those documents produced in native electronic format) all documents in your submission, preferably with a unique Bates identifier, and indicate the total number of documents in your submission.
- L. **Production of Copies.** Documents that may be responsive to more than one specification of this CID need not be submitted more than once. Legible photocopies may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of original documents may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request.
- M. **Electronic Submission of Documents:** The following guidelines refer to the production of any Electronically Stored Information ("ESI") or digitally imaged hard copy documents. Before submitting any electronic production, you must confirm with one of the Commission representatives named below that the proposed formats and media types

will be acceptable to the Commission. The FTC requests Concordance load-ready electronic productions, including DAT and OPT load files.

1. Electronically Stored Information: documents created, utilized, or maintained in electronic format in the ordinary course of business should be delivered to the FTC as follows:
 - a. Spreadsheet and presentation programs, including but not limited to Microsoft Access, SQL, and other databases, as well as Microsoft Excel and PowerPoint files, must be produced in native format with extracted text and metadata. Data compilations in Excel spreadsheets, or in delimited text formats, must contain all underlying data un-redacted with all underlying formulas and algorithms intact. All database productions (including structured data document systems) must include a database schema that defines the tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, Java, XML schemas, and other elements, including the use of any report writers and custom user data interfaces;
 - b. All ESI other than those documents described in (1)(a) above must be provided in native electronic format with extracted text or Optical Character Recognition (OCR) and all related metadata, and with corresponding image renderings as converted to Group IV, 300 DPI, single-page Tagged Image File Format (TIFF) or as color JPEG images (where color is necessary to interpret the contents); and
 - c. Each electronic file should be assigned a unique document identifier ("DocID") or Bates reference.
2. Hard Copy Documents: Documents stored in hard copy in the ordinary course of business should be submitted in an electronic format when at all possible. These documents should be true, correct, and complete copies of the original documents as converted to TIFF (or color JPEG) images with corresponding document-level OCR text. Such a production is subject to the following requirements:
 - a. Each page shall be endorsed with a document identification number (which can be a Bates number or a document control number);
 - b. Logical document determination should be clearly rendered in the accompanying load file and should correspond to that of the original document; and

- c. Documents shall be produced in color where necessary to interpret them or render them intelligible.
3. For each document electronically submitted to the FTC, you should include the following metadata fields in a standard ASCII delimited Concordance DAT file:
 - a. **For electronic mail:** begin Bates or unique document identification number ("DocID"), end Bates or DocID, mail folder path (location of email in personal folders, subfolders, deleted or sent items), custodian, from, to, cc, bcc, subject, date and time sent, date and time received, and complete attachment identification, including the Bates or DocID of the attachments (AttachIDs) delimited by a semicolon, MD5 or SHA Hash value, and link to native file;
 - b. **For email attachments:** begin Bates or DocID, end Bates or DocID, parent email ID (Bates or DocID), page count, custodian, source location/file path, file name, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file;
 - c. **For loose electronic documents** (as retrieved directly from network file stores, hard drives, etc.): begin Bates or DocID, end Bates or DocID, page count, custodian, source media, file path, filename, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file; and
 - d. **For imaged hard copy documents:** begin Bates or DocID, end Bates or DocID, page count, source, and custodian; and where applicable, file folder name, binder name, attachment range, or other such references, as necessary to understand the context of the document as maintained in the ordinary course of business.
4. If you intend to utilize any de-duplication or email threading software or services when collecting or reviewing information that is stored in your computer systems or electronic storage media, or if your computer systems contain or utilize such software, you must contact a Commission representative named below to determine whether and in what manner you may use such software or services when producing materials in response to this Request.
5. Submit electronic productions as follows:
 - a. With passwords or other document-level encryption removed or otherwise provided to the FTC.

- b. As uncompressed electronic volumes on size-appropriate, Windows-compatible, media.
- c. All electronic media shall be scanned for and free of viruses.
- d. Data encryption tools may be employed to protect privileged or other personal or private information. The FTC accepts TrueCrypt, PGP, and SecureZip encrypted media. The passwords should be provided in advance of delivery, under separate cover. Alternate means of encryption should be discussed and approved by the FTC.
- e. Please mark the exterior of all packages containing electronic media sent through the U.S. Postal Service or other delivery services as follows:

**MAGNETIC MEDIA – DO NOT X-RAY
MAY BE OPENED FOR POSTAL INSPECTION.**

- 6. All electronic files and images shall be accompanied by a production transmittal letter which includes:
 - a. A summary of the number of records and all underlying images, emails, and associated attachments, native files, and databases in the production; and
 - b. An index that identifies the corresponding consecutive document identification number(s) used to identify each person's documents and, if submitted in paper form, the box number containing such documents. If the index exists as a computer file(s), provide the index both as a printed hard copy and in machine-readable form (provided that a Commission representative named below determines prior to submission that the machine-readable form would be in a format that allows the agency to use the computer files). The Commission counsel named above will provide a sample index upon request.

A Bureau of Consumer Protection Production Guide is available upon request from a Commission representative named below. This guide provides detailed directions on how to fully comply with this instruction.

- N. **Sensitive Personally Identifiable Information.** If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please contact us before sending those materials to discuss ways to protect such information during production.

For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

- O. **Information Identification.** Each specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification(s) or subspecification(s) to which it is responsive.
- P. **Commission Representatives.** Any questions you have relating to the scope or meaning of anything in this CID should be directed to Kristin Cohen at (202) 326-2276 or Lisa Schifferle at (202) 326-3377.

III. INTERROGATORIES

Demand is made for the following information:

- 1. Identify
 - a. each Wyndham entity's total number of employees and total annual revenues;
 - b. each Wyndham-franchised hotel, its mailing address, the date on which it first entered into a franchise agreement with Wyndham Hotels, and, if applicable, the date on which its franchise agreement was terminated; and
 - c. each Wyndham-managed hotel, its mailing address, the date on which it first entered into a management agreement with Hotel Management, and, if applicable, the date on which its management agreement was terminated.
- 2. Provide a high-level diagram (or diagrams) that sets out the components of each computer network used by Wyndham Hotels and Hotel Management to store and process personal information, including any network hosted by Wyndham Hotels or Hotel Management on behalf of any Wyndham-branded hotel, and any network that would allow access to the network(s) of any Wyndham-branded hotel that stores and processes personal information. To the extent your network(s) changed throughout the applicable time period, you should provide separate diagrams for the time periods immediately

preceding each data breach identified in response to Interrogatory Specification 16. In addition, provide a narrative that describes the components in detail and explains their functions and how they operate. Such diagram(s) and description shall include the location (within the network) of: computers; servers; firewalls; routers; internet, private line, and other connections; connections to other internal and external networks; virtual private networks; remote access equipment (such as wireless access points); websites; and security mechanisms and devices (such as intrusion detection systems).

3. Describe in detail how the Wyndham-branded hotels' networks are connected to any Company network(s), including all connections between the Company's central reservation system(s), its guest loyalty database(s), and the Wyndham-branded hotels. Your response should explain whether and how the Wyndham-branded hotels may access the central reservation system(s) or guest loyalty database(s), describe the personal information contained in each, and describe any access controls in place to limit access to the central reservation system or guest loyalty database.
4. Describe the process(es) used by Wyndham Hotels and Hotel Management, on behalf of themselves or any Wyndham-branded hotel, to obtain authorization for payment card transactions ("card authorization"). This description should include:
 - a. the complete transmission or flow path for authorization requests and responses and the underlying information for each network involved in card authorization, starting with the merchant to whom a card is presented to pay for a purchase and including each intermediary on the path (including, but not limited to: bank associations; acquiring, issuing, and other banks; Wyndham Hotels or Hotel Management; third-party processors; merchant servicers; independent sales organizations; and other entities), and ending with receiving the response to the authorization request;
 - b. each portion, if any, of the transmission or flow paths described in response to Interrogatory Specification 4a, above, where authorization requests, authorization responses, or the underlying personal information were transmitted in clear text, as well as the time period during which the requests, responses, and information were transmitted in clear text;
 - c. identification of the system(s), computer(s), or server(s) used to aggregate authorization requests in whole or in part and transmit them to bank associations and banks ("card authorization server"), and, for each server, the application(s) used for card authorization and the services enabled on the server, and a description of how the server has been protected from unauthorized access (such as protected by its own firewall); and

- d. where authorization requests and responses and underlying personal information are stored or maintained (such as by being stored on a card authorization server or written to transaction logs located elsewhere on a network), as well as how stored or maintained requests, responses, and information have been protected from unauthorized access and the length of time they are retained.
5. Describe in detail Wyndham Worldwide's role in the Information Security Programs of The Hotel Group, Wyndham Hotels, Hotel Management, the Wyndham-franchised hotels, and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following:
 - a. Wyndham Worldwide's role in developing and implementing each entity's Information Security Program;
 - b. the training Wyndham Worldwide provides to each entity related to the protection of personal information, including PCI DSS compliance;
 - c. all policies, practices, and procedures relating to Wyndham Worldwide's audits, assessments, and oversight of each entity's Information Security Program, including any role it has had in ensuring each entity's compliance with PCI DSS;
 - d. Wyndham Worldwide's role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;
 - e. Wyndham Worldwide's role in providing payment card authorization for each entity; and
 - f. the Wyndham Worldwide employee(s) responsible for overseeing each entity's Information Security Program.
6. Describe in detail The Hotel Group's role in the Information Security Programs of Wyndham Hotels, Hotel Management, the Wyndham-franchised hotels and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following:
 - a. The Hotel Group's role in developing and implementing each entity's Information Security Program;
 - b. the training The Hotel Group provides to each entity related to the protection of personal information, including PCI DSS compliance;

- c. all policies, practices, and procedures relating to The Hotel Group's audits, assessments, and oversight of each entity's Information Security Program, including any role it has had in ensuring each entity's compliance with PCI DSS;
 - d. The Hotel Group's role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;
 - e. The Hotel Group's role in providing payment card authorization for each entity; and
 - f. The Hotel Group employee(s) responsible for overseeing each entity's Information Security Program.
7. Describe in detail Wyndham Hotels' role in the Information Security Programs of Hotel Management, the Wyndham-franchised hotels, and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following:
- a. Wyndham Hotels' role in developing and implementing each entity's Information Security Program;
 - b. the training Wyndham Hotels provides to each entity related to the protection of personal information, including PCI DSS compliance;
 - c. all policies, practices, and procedures relating to Wyndham Hotels' audits, assessments, and oversight of each entity's Information Security Program, including any role it has had in ensuring each entity's compliance with PCI DSS;
 - d. Wyndham Hotels' role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;
 - e. Wyndham Hotels' role in providing payment card authorization for each entity; and
 - f. the Wyndham Hotels employee(s) responsible for overseeing each entity's Information Security Program, his title(s), and the total number of employees responsible for handling information security.
8. Identify and describe in detail Hotel Management's role in the Information Security Program of the Wyndham-franchised hotels and the Wyndham-managed hotels,

including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following:

- a. Hotel Management's role in developing and implementing each hotel's Information Security Program;
 - b. the training Hotel Management provides to each hotel related to the protection of personal information, including PCI DSS compliance;
 - c. all policies, practices, and procedures relating to Hotel Management's audits, assessments, and oversight of each hotel's Information Security Program, including any role it has had in ensuring each hotel's compliance with PCI DSS;
 - d. Hotel Management's role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;
 - e. Hotel Management's role in providing payment card authorization for each hotel; and
 - f. a list of all Hotel Management employee(s) responsible for overseeing each hotel's Information Security Program.
9. Identify and describe in detail the 2009 decision that Wyndham Worldwide would assume responsibility from The Hotel Group for Wyndham Hotels' Information Security Program, as described in the Access Letter Response (the "decision"). Your answer should include, but not be limited to, the following:
- a. which Company personnel were involved in the decision making process;
 - b. who approved the decision;
 - c. all reasons for the decision; and
 - d. any personnel changes as a result of the decision, including any transfer of personnel employed by one Wyndham entity to another Wyndham entity as a result of the change.
10. Describe in detail the role of each Wyndham entity in managing the property management systems and payment processing applications of the Wyndham-branded hotels, including when and how those roles changed throughout the applicable time period and how those roles differed between the Wyndham-franchised hotels and the

Wyndham-managed hotels. Your answer should include, but not be limited to, a description of the following (separately for each Wyndham entity):

- a. the types of property management systems and payment processing applications used by the Wyndham-branded hotels (including, but not limited to, Opera, Fidelio, and ProtoBase);
 - b. the guidance provided to the Wyndham-branded hotels regarding the types of hardware and software required for their property management systems or payment processing applications, including any needed upgrades;
 - c. the support provided to the Wyndham-branded hotels in configuring their property management systems or payment processing applications;
 - d. the oversight provided of Micros and Southern DataComm in installing and configuring the Wyndham-branded hotels' property management systems or payment processing applications;
 - e. the extent to which any Wyndham entity put any property management system or payment processing application, including Protobase, into debugging mode or was aware that such systems were running in debugging mode; and
 - f. any other services performed in each Wyndham entity's management of the Wyndham-branded hotels' property management systems or payment processing applications.
11. Identify any Wyndham-branded hotels that failed to sign the Technology Addendum to their franchise or management agreement in 2009, as described in the Access Letter Response, and state (1) if given, the reason provided by the hotel for not signing the Technology Addendum; (2) whether the franchise or management agreement with the hotel was terminated; (3) the date of such termination; and (4) whether a hotel's failure to sign the Technology Addendum resulted in any other consequences and, if so, state what the consequences were.
12. Separately for each Wyndham entity and for the Wyndham-branded hotels, provide the following information (including any changes that occurred throughout the applicable time period):
- a. all practices to control, monitor, and record authorized and unauthorized access to personal information on its network(s);
 - b. the frequency and extent to which network users receive information security training or security awareness materials;

- c. whether and, if so, when risk assessment(s) were performed to identify risks to the security, integrity, and confidentiality of personal information on its network(s);
 - d. the manner in which it or another person or entity tests, monitors, or evaluates the effectiveness of its Information Security Program, including practices to ensure that all persons or entities that obtain access to personal information are authorized to do so and use the information for only authorized purposes.
 - e. when testing, monitoring, or evaluation activities were conducted and all changes made to security practices on the network(s) based upon such testing, monitoring, or evaluation;
 - f. all other security procedures, practices, policies, and defense(s) (such as access controls or encryption) in place to protect personal information from unauthorized access while stored on the network, transmitted within the network or between networks, or processed on the network, including the date on which it was implemented; and
 - g. identify the employee(s) responsible for implementing its Information Security Program.
13. For each risk assessment identified in response to Interrogatory Specification 12c, as well as any assessment(s) performed by Fishnet Security, Inc. beginning in 2005 of Wyndham Hotels' computer network(s) or Information Security Program, identify:
- a. the date of the assessment and the name and title of the person(s) responsible for conducting and overseeing the assessment;
 - b. the steps taken in conducting the assessment;
 - c. the specific risks identified in the assessment; and
 - d. how and by whom each risk was addressed.
14. For each Wyndham Hotels and Hotel Management Service Provider:
- a. identify the Service Provider;
 - b. identify the types of personal information that Wyndham Hotels and Hotel Management allow the Service Provider to access;

- c. describe the manner and form of access (such as physical access to Company offices or remote access to computer systems, including administrative access);
 - d. state the purpose(s) for such access; and
 - e. describe how the Company monitors the Service Provider to confirm that it has implemented and maintained security safeguards adequate to protect the confidentiality and integrity of personal information.
15. Describe in detail the specific technical, administrative, and physical safeguards taken to re-architect and upgrade the Wyndham Hotels' Phoenix Data Center in 2009 as described in the Access Letter Response, including, but not limited to, the following:
- a. building a new security infrastructure;
 - b. segmenting the Wyndham Hotels' Phoenix data center environment from the Wyndham-branded hotel properties' networks;
 - c. expanding Wyndham Hotels' global threat management system to include critical hotel property systems;
 - d. changing the remote access process;
 - e. making process improvements for account administrative authorization;
 - f. ensuring that all internal system administrators now have two-factor authentication for remote access from outside the Wyndham Hotels network;
 - g. creating a holistic view of the Wyndham Hotels' environment; and
 - h. any upgrades made to Wyndham Hotels' virus monitoring.
16. Identify each data breach that is known to have occurred since January 1, 2008, and, for each data breach identified, describe in detail how, when, and through whom the Company first learned about the breach.
17. Identify all consultants, agents, or other entities that assisted any Wyndham entity in connection with any actions it took relating to the data breaches identified in response to Interrogatory Specification 16. For each such entity, state on which Wyndham entity's behalf the entity was retained and provide a brief description of the services rendered.
18. Describe in detail any network user account lockouts related to any data breach identified in response to Interrogatory Specification 16, and the Company's investigations of any

such lockouts, including but not limited to, when the investigation was initiated, the personnel notified, and the steps taken to determine whether an intruder had gained access to the network(s).

19. For each data breach identified in response to Interrogatory Specification 16, identify the name and location of each computer system on which personal information was or may have been accessed as a result of each such breach, and for each such system describe:
 - a. the type(s) and amount(s) of potentially compromised personal information;
 - b. any report of subsequent unauthorized use of compromised personal information alleged in any way to be linked to each instance of unauthorized access, including, but not limited to, the number of instances where payment cards were alleged to have been used without the card holder's authorization, the dates of such use, and the amounts charged or debited;
 - c. each known or suspected intruder;
 - d. the manner by which each intruder obtained access to the compromised personal information, including security practices that permitted or may have permitted the data breach to occur;
 - e. the time period over which: (1) the data breach occurred; and (2) personal information was or may have been accessed;
 - f. each security measure implemented in response to the data breach, including the date on which it was implemented; and
 - g. sanctions imposed in response to the data breach.

20. For each data breach identified in response to Interrogatory Request 16, describe in detail any investigations conducted to determine the likely cause of the breach or the security vulnerabilities that may have led to the breach, including investigations conducted by any Wyndham entity, as well as those conducted on behalf of the Card Associations. Your response should include, but not be limited to, the following:
 - a. a description of the findings of any such investigation;
 - b. a description of any disputes the Company has with the findings of any such investigation;
 - c. a description of the role any Wyndham entity played in overseeing any investigation conducted of a Wyndham-branded hotel; and

- d. identification of any Company employee(s) responsible for overseeing any such investigations.
21. For each policy or statement submitted in response to Document Specification 15, identify the date(s) when it was adopted or made, and describe all means by which it was distributed.
 22. Identify all officers and members of the Board of Directors of each Wyndham entity during the applicable time period. In doing so, identify all officers or Board members of any Wyndham entity who are also serving or have ever served as officers or Board members of another Wyndham entity. For each such person, state for which Wyndham entities he or she served as an officer or Board member and the time period during which he or she served in such role.
 23. Describe the extent to which accounting, managerial, marketing, distributing, human resources, information security, legal and other functions or facilities are shared or inter-related between each Wyndham entity. Your response should include, but not be limited to, a description of whether any Wyndham entity pays on behalf of any other Wyndham entity (1) its payroll, or (2) the premiums for any director or officer insurance coverage, and whether any Wyndham entity transfers or otherwise allocates for accounting purposes any consideration to another Wyndham entity in exchange for providing any information security-related service.
 24. For any document request specification for which there are documents that would be responsive to this CID, but which were destroyed, mislaid, transferred, deleted, altered, or over-written:
 - a. identify the document;
 - b. state the date such document was destroyed, mislaid, transferred, deleted, altered, or overwritten;
 - c. describe the circumstance under which such document was destroyed, mislaid, transferred, deleted, altered, or overwritten; and
 - d. identify the person authorizing such action.
 25. Identify the person(s) responsible for preparing the response to this CID, and describe in detail the steps taken to respond to this CID, including instructions pertaining to document (written and electronic) and information preservation. Where oral instructions were given, identify the person who gave the instructions and describe the content of the instructions and the person(s) to whom the instructions were given. For each specification, identify the individual(s) who assisted in preparing the response, with a

listing of the persons (identified by name and corporate title or job description) whose files were searched by each person.

26. To the extent that any information provided in the Access Letter Response may require updating or is otherwise incomplete or inaccurate, supplement your response.

V. DOCUMENTARY MATERIALS

Demand is made for the following documents:

1. Each different franchise and management contract with a Wyndham-branded hotel that governs the storing and processing of personal information, including all addenda to such contracts.
2. All documents provided to Wyndham-branded hotels related to information technology or information security, including but not limited to: training materials; operation manuals; system standards; information security policies; PCI DSS compliance documents; and documents related to property management system or payment application hardware, software, or configuration requirements.
3. Documents sufficient to describe the relationship between the networks of the Wyndham entities, including but not limited to: who supplies each Wyndham entity with its network(s); who owns the network(s); who maintains the network(s); who sets standards for the network(s); who monitors the network(s); and who is responsible for information security on the network(s).
4. Documents sufficient to describe each Wyndham entity's role in managing the Wyndham-branded hotels' computer networks, including but not limited to: who supplies each Wyndham-branded hotel with its network(s); who owns the network(s); who maintains the network(s); who sets standards for the network(s); who monitors the network(s); who is responsible for information security on the network(s); and how the Company's role is different between Wyndham-franchised hotels and Wyndham-managed hotels.
5. Documents sufficient to describe the Company's relationship with any property management system or payment processing vendor, including but not limited to Micros, Southern DataComm, and Elavon, related to the installation, configuration, operation, or technical support of the property management systems or payment processing applications for the Wyndham-branded hotels and Wyndham Hotels' central reservation system. Your response should include, but not be limited to, all contracts between the Company and Micros, Southern DataComm, and Elavon related to property management systems or payment processing applications.

6. Documents sufficient to describe the Information Security Program of each Wyndham entity, including but not limited to, documents describing:
 - a. access controls in place, including who has access to personal information on their network(s), including any Service Providers or Wyndham-branded hotels;
 - b. physical or electronic information security measures taken to protect personal information, including but not limited to practices to monitor and record unauthorized access (such as intrusion detection systems), password requirements, employee turnover procedures, procedures for transporting personal information, and log retention policies;
 - c. the means by which each Wyndham entity's computer network(s) may be accessed externally, including by Service Providers or Wyndham-branded hotels;
 - d. the technical configurations of devices and programs it uses to implement its Information Security Program, including but not limited to configurations of firewalls or other means used to control, monitor, or record access to personal information;
 - e. completed or planned testing, monitoring, or evaluation of its Information Security Program; and
 - f. information security training provided to network users (such as employees, Wyndham-branded hotels, and Service Providers) regarding the Information Security Program.
7. All documents that assess, evaluate, question, challenge, or contest the effectiveness of any Wyndham entity's or Wyndham-branded hotel's Information Security Program, or recommend changes to it, including, but not limited to internal and external security assessments, plans, reports, studies, audits, audit trails, evaluations, and tests. Your response should include all documents that relate to each risk assessment described in response to Interrogatory Specification 13, including but not limited to a copy of each internal and external report that verifies, confirms, challenges, questions, or otherwise concerns such assessment.
8. For each Service Provider identified in response to Interrogatory Specification 14, all provisions of contracts with the Company relating to the handling of personal information, and all other policies, procedures, or practices that relate to each Service Provider's handling of personal information, including any policies or practices related to granting the Service Provider administrative access to any Company network.

9. For each data breach identified in response to Interrogatory Specification 16, all documents prepared by or for the Company that identify, describe, investigate, evaluate, or assess such breach, including but not limited to preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in each breach; reports of penetration and gap analysis; logs that record the intruder's steps in accessing or using compromised personal information; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was configured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of each breach prepared internally and by third-parties; and other records relating or referring to each breach, including minutes or notes of meetings attended by the Company's personnel and documents that identify the intruder(s).
10. All communications between the Company or a Wyndham-branded hotel and Micros, Southern DataComm, or Elavon related to:
 - a. the installation or configuration of any property management system or payment processing application;
 - b. any data breach;
 - c. remote access to any network identified in response to Interrogatory Specification 2 or to the network(s) of any Wyndham-branded hotel;
 - d. the use of debugging in any application; and
 - e. the use of passwords, including descriptions of who is responsible for setting passwords and password requirements.
11. All communications between the Company and the Wyndham-branded hotels related to:
 - a. any data breach, and including any documents referencing fines or assessments from any Card Association;
 - b. the use of debugging in any property management system or payment processing application;
 - c. PCI DSS compliance; and

- d. the use of passwords on any application, including who is responsible for setting passwords and password requirements for accessing the Company's central reservation system or related to the Wyndham-branded hotels' property management systems or payment processing applications.
12. All communications between the Company or a Wyndham-branded hotel and any Card Association related to any data breach identified in response to Interrogatory Specification 16.
13. All communications between the Company or a Wyndham-branded hotel and any consultant, agent, or other entity identified in response to Interrogatory Specification 17 relating to information security or to any data breach.
14. Documents sufficient to describe the Company's quality assurance program for inspecting the Wyndham-branded hotels' compliance with their franchise or management contracts, including but not limited to, documents that describe:
 - a. how often each Wyndham-branded hotel is inspected;
 - b. which Wyndham entity is responsible for conducting the inspections;
 - c. how the quality assurance program differs between Wyndham-franchised hotels and Wyndham-managed hotels;
 - d. criteria for determining whether and how often to inspect each Wyndham-branded hotel; and
 - e. any inspections done of Wyndham-branded hotels related to either information technology or information security.
15. All policies, claims, and statements made to consumers by or for the Company regarding the collection, disclosure, use, storage, destruction, and protection of personal information, including any policies, claims, or statements relating to the security of such information.
16. All documents that relate to actual or potential harm to consumers or claims of harm made by consumers that are based on any data breach identified in response to Interrogatory Specification 16. Responsive documents should include, but not be limited to:
 - a. documents that assess, identify, evaluate, estimate, or predict the number of consumers that have, or are likely to, suffer fraud, identity theft, or other harm; claims made against the Company or any Wyndham-branded hotel for fraud,

identity theft, or other harm, such as by affidavits filed by consumers; and documents that assess, identify, evaluate, estimate, or predict the dollar amount of fraud, identity theft, or other costs (such as for increased fraud monitoring or providing fraud insurance) attributable to each such incident; and

- b. documents that relate to investigations of or complaints filed with or against the Company or any Wyndham-branded hotel relating to each data breach, including, but not limited to, private lawsuits, correspondence with the Company or any Wyndham-branded hotel, and documents filed with federal, state, or local government agencies, federal or state courts, and Better Business Bureaus.
17. All contracts and memoranda relating to the transfer of information security responsibilities for Wyndham Hotels from The Hotel Group to Wyndham Worldwide, and all contracts between any Wyndham entities relating to responsibility for information security.
 18. All minutes of Board of Directors meetings, executive committee meetings, or audit committee meetings of each Wyndham entity during the applicable time period.
 19. Documents sufficient to show the Company's policies and procedures relating to the retention and destruction of documents.

Exhibit A



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Lisa W. Schifferle
Attorney
Division of Privacy & Identity Protection

Direct Dial: 202.326.3377
Fax : 202.326.3768
E-mail: lschifferle@ftc.gov

April 8, 2010

BY EMAIL AND FEDERAL EXPRESS

Kirsten Hotchkiss
Senior Vice President - Legal and Assistant Secretary
Wyndham Hotels and Resorts, LLC
7 Sylvan Way
Parsippany, NJ 07054

Dear Ms. Hotchkiss:

As stated in my voice-mail message earlier today, the staff of the Federal Trade Commission ("Commission") is conducting a non-public investigation into Wyndham Hotels and Resorts, LLC's ("Wyndham") compliance with federal laws governing information security. According to recent news reports and statements issued by Wyndham,¹ sensitive personal information (including credit card information) of Wyndham's customers was obtained from Wyndham's computer networks by unauthorized individuals on three separate occasions since July 2008 (hereinafter "the three breaches"). We seek to determine whether Wyndham's information security practices comply with Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits deceptive or unfair acts or practices, including misrepresentations about security and unfair security practices that cause substantial injury to consumers.²

¹ See, e.g. www.pcworld.com, *Wyndham Hotels Hacked Again* (Feb. 26, 2010), http://www.pcworld.com/businesscenter/article/wyndham_hotels_hacked_again.html; www.computerworld.com, *Losing Sleep over Three Data Breaches in a Year* (Mar. 5, 2010), http://www.computerworld.com/s/article/9166538/Losing_sleep_over_three_data_breaches_in_a_year.html; Wyndham Hotels and Resorts (Feb. 2010), http://www.wyndhamworldwide.com/customer_care/data-claim-faq.cfm.

² 15 U.S.C. § 45 *et seq.*

As part of our review, we ask that you provide us with the information and documents listed below on or before **May 10, 2010**. Please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. After we receive the information and documents, we will invite you to meet with Commission staff in our Washington, D.C. office or by telephone to further discuss this matter. In preparing your response:

- For purposes of this letter, "Wyndham" shall include Wyndham Hotels and Resorts, LLC, its parents, subsidiaries, divisions, affiliates, franchisees, hotels managed by franchisees that use the Wyndham trade name, and agents.
- Please provide all responsive documents within the possession, custody and control of Wyndham.
- Please submit *complete* copies of all documents and materials requested, even if you deem only a part of the document to be responsive.
- If any documents are undated, please indicate the date on which they were prepared or received by Wyndham.
- Please Bates stamp your response and itemize it according to the numbered paragraphs in this letter. If you have previously submitted documents, please refer to Bates number(s) in your itemized response to prevent unnecessary duplication.
- If you do not have documents that respond to a particular request, please submit a written statement in response. If a document provides only a partial response, please submit a written statement which, together with the document, provides a complete response.
- If you decide to withhold responsive material for any reason, including an applicable privilege or judicial order, please notify us before the date set for response to this request and submit a list of the items withheld and the reasons for withholding each.
- For purposes of this letter, the term "personal information" means individually identifiable information from or about an individual consumer, including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) a driver's license number; (g) financial account information, including account numbers or identifiers, and credit, debit, and/or ATM card information such as card number, expiration date, and data stored on a card's magnetic stripe; (h) a persistent identifier, such as a customer number held

in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information from or about an individual consumer that is combined with any of (a) through (h) above.

- Please note that we do not wish to receive files containing any individual consumer's Social Security or driver's license number, or financial account information. If you have responsive documents that include such information, please redact that information before providing us with the documents.
- We may seek additional information from you at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested below, but also any other information that concerns, reflects, relates to this matter, including files and information stored electronically, whether on computers, computer disks and tapes, or otherwise) until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.³ This request is not subject to the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.
- A responsible corporate officer or manager of Wyndham shall sign the responses and certify that the documents produced and responses given are complete and accurate.

REQUEST FOR DOCUMENTS AND INFORMATION

Please provide the documents and information requested below.⁴ Unless otherwise indicated, the time period covered by these requests is from **January 1, 2008** through the date of full and complete production of the documents and information requested.

³ Failure to retain documents that may be relevant to this matter may result in civil or criminal liability. 15 U.S.C. § 50.

⁴ For purposes of this letter the word "any" shall be construed to include the word "all," and the word "all" shall be construed to include the word "any." The word "or" shall be construed to include the word "and" and the word "and" shall be construed to include the word "or." The word "each" shall be construed to include the word "every," and the word "every" shall be construed to include the word "each." The term "document" means any preexisting written or pictorial material of any kind, regardless of the medium in which such material was created, and regardless of the method by which it is stored (e.g., computer file, computer disk or tape, or microfiche).

General Information

1. Identify the complete legal name of Wyndham and all other names under which it does, or has done, business, its corporate mailing address, and the date and state of incorporation.
2. Identify and describe Wyndham's parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchisees, operations under assumed names, and entities over which it exercises supervision or control. For each such entity, describe in detail the nature of its relationship to Wyndham and provide copies of any contracts regarding its relationship with Wyndham.
3. Provide documents sufficient to identify and describe in detail Wyndham's business. The response should include but not be limited to: (a) the products and services Wyndham (including but not limited to hotels managed by franchisees that use the Wyndham trade name) offers, sells, or otherwise provides to customers; and (b) information identifying, annually, total revenue and total number of employees.
4. Identify the name, location, and operating system of each computer network Wyndham (including but not limited to its franchisees or other related entities) used to store, maintain, process, transmit, handle, or otherwise use (collectively hereinafter, "store and process") personal information (such as to prepare, send, and receive authorization requests for credit and debit card transactions) as of January 1, 2008.
5. For each network identified in the response to Request 4, above:
 - (a) identify the type(s) of personal information stored and processed on the network, the source of each type of information (including, but not limited to: credit or debit cards; information provided by customers to obtain gifts or rewards; and information provided by third parties); and describe in detail how each type of information is stored and processed by Wyndham;
 - (b) provide:
 - (1) blueprints and diagrams setting out in detail the components, topology, and architecture of the network. Responsive documents should include, but not be limited to: documents that identify and locate the components of the network, such as computers; POS devices; cash registers; remote access equipment (such as wireless access points); servers; firewalls; routers; internet, private line, and other connections; connections to other Wyndham networks and outside networks; and

security mechanisms and devices (such as intrusion detection systems);
and

(2) a narrative that describes in detail the components of the network and explains the functions of the components, and how the components operate together on the network;

- (c) provide documents setting out, and describe in detail, the security procedures, practices, policies, and defense(s) (such as access controls or encryption) in place to protect personal information from unauthorized access while stored on the network, transmitted within the network or between networks, and/or processed on the network;
- (d) provide all documents that concern, relate, or refer to security vulnerabilities in the network, including, but not limited to, documents identifying vulnerabilities, documents setting out and explaining the measures implemented to address the vulnerabilities, and communications, such as emails, that assess, question, or describe the state of security, warn of vulnerabilities, or propose or suggest changes in security measures; and
- (e) provide the name(s), title(s), and contact information of the individual(s) responsible for creating, designing, managing, securing, and updating the network.

The responses to each subpart of this Request should describe in detail each material change or update that has been made that concerns, refers, or relates to the subpart, as well as the date the change or update was implemented and the reason(s) for the change or update. If each network has the same standard framework, then you may provide one example rather than providing repeated copies of the same standard network.

6. Describe in detail, and provide documents setting out, the process(es) Wyndham (including but not limited to its franchisees or any other related entities outlined in response to Request #2) uses to provide authorization for credit or debit card transactions (“card authorization”). The response should:

- (a) set forth the complete transmission or flow path for authorization requests and responses and the underlying information for each network involved in any way in card authorization, starting with the entity to whom a card is presented to pay for a purchase and including each intermediary on the path (including, but not limited to Visa, MasterCard, American Express, Discover [hereinafter collectively, “bank associations”]; acquiring, issuing, and other banks; Wyndham; third-party processors; merchant servicers; independent sales organizations; and

other entities) and final destination, and ending with receiving the response to the authorization request;

- (b) identify each portion of the transmission or flow paths set out in the response to Request 6(a), above, where authorization requests, authorization responses, or the underlying personal information are transmitted in clear text, if any, as well as the time period during which the requests, responses and information were transmitted in clear text;
- (c) identify the system(s), computer(s), or server(s) used to aggregate authorization requests in whole or in part and transmit them to bank associations and banks ("card authorization server"), and, for each server, identify the application(s) used for card authorization and the services enabled on the server, and describe in detail how the server has been protected from unauthorized access (such as protected by its own firewall);
- (d) describe in detail how and where authorization requests and responses and underlying personal information are stored or maintained (such as by being stored on a card authorization server or written to transaction logs located elsewhere on a network), as well as how stored or maintained requests, responses, and information have been protected from unauthorized access; and
- (e) identify and describe the number of authorization requests and responses that Wyndham received, forwarded, processed, stored, or transmitted for each month over the period in question, as well as the type of card presented to the merchant (such as credit or debit) and the disposition of the request (such as approved, declined, not completed, not authorized, or other classification, description, or category).

Information About the Three Breaches

In this section entitled "Information About the Three Breaches," please respond to each of the questions breach by breach. In other words, answer Requests #7-12 for the first breach (July-August 2008), then answer Requests #7-12 for the second breach (March-May 2009), and then answer Request #7-12 for the third breach (October 2009-January 2010).

- 7. For each breach, describe in detail and produce documents sufficient to identify how and when Wyndham first learned about the breach.
- 8. Provide all documents prepared by or for Wyndham that identify, describe, investigate, evaluate, or assess: (a) how each breach occurred; (b) the time period over which it occurred; (c) where each breach began (*e.g.*, what the point of entry was and where it was located on the network); and (d) the path the

intruder followed from the point of entry to the information compromised and then in exporting or downloading the information (including all intermediate steps).

Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in each breach; reports of penetration and gap analysis; logs that record the intruder's steps in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was configured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of each breach prepared internally and by third-parties; and other records relating or referring to each breach, including minutes or notes of meetings attended by Wyndham's personnel and documents that identify the attacker(s).

9. Identify the name and location of each computer network on which personal information may have been accessed as a result of each breach, and for each such network describe in detail and provide all documents that relate to:
 - (a) the type(s) (*e.g.*, consumer's name, address, and payment card number, expiration date, and security code) and amount(s) of personal information that was or may have been obtained, including but not limited to the number of credit and/or debit card numbers;
 - (b) any subsequent unauthorized use of credit and/or debit cards alleged in any way to be linked to each instance of unauthorized access, including, but not limited to, the number of instances where credit and/or debit cards were used without the card holder's authorization, the dates of such use, and the amounts charged or debited.

Responsive documents should include, but not be limited to: fraud reports, alerts, or warnings issued by bank associations, banks, or other entities; lists identifying credit, debit, and other types of cards that have been used without authorization or may have been exposed by each breach as well as the issuing banks; documents that assess, identify, evaluate, estimate, or predict the amount of fraudulent purchases resulting from each breach; claims made against Wyndham's acquiring bank(s) under bank network alternative dispute resolution programs (*e.g.*, pre-compliance and compliance actions), and the resolution of any such claims; claims made against Wyndham by banks that issued cards that

have been used for unauthorized purchases (such as by demand letters); claims of fraud and/or identity theft, including, but not limited to, affidavits filed by consumers with their banks; and documents that assess, identify, evaluate, estimate, or predict the number of credit, debit, and other types of cards that have been cancelled and/or reissued, the cost per card and in total of cancelling and/or reissuing cards, and additional costs to Wyndham and/or third parties, attributable to each breach (such as for increased monitoring for fraud or providing fraud insurance to consumers affected by each breach);

- (c) the security procedures, practices, policies, and defenses in place when the first instance of each breach occurred as well as any changes to those security procedures, practices, policies, or defenses made thereafter;
- (d) each action Wyndham has taken in response to learning about the unauthorized access to personal information (*e.g.*, notifying consumers or law enforcement, improving security), including when the action was taken; and
- (e) investigations of or complaints filed with or against Wyndham that concern unauthorized access to personal information, including but not limited to correspondence with Wyndham and documents filed with: Federal, State, or local government agencies; Federal or State courts; and Better Business Bureaus.

10. According to news articles, at least one breach involved a hacker accessing a Wyndham data center through a franchisee.⁵

- (a) Identify which franchisees, subsidiaries, or data centers were involved in each of the three breaches.
- (b) For each such franchisee, subsidiary or data center identified in response to Request 10a, describe and provide documents relating to Wyndham's requirements regarding such entity's compliance with Wyndham's security practices.
- (c) For each such franchisee, subsidiary or data center identified in response to Request 10a, describe and provide documents relating to the network relationship between the entity and Wyndham, including but not limited to: who supplies such entity with its networks and/or who owns the

⁵ See, *e.g.* [www.networkworld.com](http://www.networkworld.com/news/2009/021809-hackers-steal-thousands-of-wyndham-credit-card-numbers.html), *Hackers steal thousands of Wyndham credit card numbers* (Feb. 18, 2009), <http://www.networkworld.com/news/2009/021809-hackers-steal-thousands-of-wyndham-credit-card-numbers.html>.

networks; who maintains those networks; who sets security standards for those networks; who monitors those networks; who is responsible for security on those networks; and who is authorized to have access to those networks.

11. According to a statement by Wyndham,⁶ at least one breach may have affected consumers in countries outside of the United States.
 - (a) Describe in detail and provide documents sufficient to identify whether non-U.S. consumers' personal information was or may have been obtained and, if so, the types and amounts of information that was or may have been obtained; the country where the information was originally collected; and whether the information was originally collected by, came from, or was sent to an entity in a member country of the European Union.
 - (b) State whether Wyndham is a certified Safe Harbor company and, if so, identify the date of certification and provide all documents and information used by Wyndham as part of its application for certification under the program.
 - (c) Provide documents sufficient to identify, and describe in detail: all networks located outside of the United States used by Wyndham to store and process personal information; the physical location(s) of each network; and the function(s) and business purpose(s) of each network; and
 - (d) For each system identified in response to Request 11(c), above, describe in detail the extent and nature of any interconnection or interface with Wyndham networks located in the United States.
12. For each of the three breaches, identify how (such as by public announcement or individual breach notification letter), when, how many, and by whom customers were notified that their information was or may have been obtained without authorization. If notification has been made, explain why notification was made (*e.g.*, compelled by law) and provide a copy of each substantively different notification. If notification was not provided as soon as Wyndham became aware of each breach or was not provided to all affected customers or at all, explain why not.

⁶ See *supra* footnote 1. According to the FAQs on Wyndham's website, "the customers represent a cross-section of Wyndham's global customer base."

Other Information

13. Describe and provide copies of each different policy adopted and statement made by Wyndham to consumers regarding the collection, disclosure, use, and protection of their personal information or customer information, including any policies and statements relating to the privacy or security of such information, and for each policy or statement, identify the date(s) when it was adopted or made, and describe all means by which it was distributed.
14. Describe in detail and provide documents sufficient to identify any other instances (besides the three breaches) of unauthorized access to Wyndham's computer system of which you are aware, as well as the types of information accessed without authorization and when the unauthorized access occurred.

In addition to these categories of documents and information, please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. Any materials you submit in response to this request, and any additional information provided it is marked "Confidential," will be given confidential treatment.⁷ We may also seek additional information at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested above, but also any other information relating to this matter, including files and information stored on computers or on computer disks and tapes) until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.⁸ This request is not subject to the requirements of the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.

Please send all documents and information to: Lisa W. Schifferle, Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Avenue, NW, Mail Stop NJ-3137, Washington, D.C. 20580. Due to extensive delays resulting from security measures taken to ensure the safety of items sent via the U.S. Postal Service, we would very much appreciate receiving these materials via Federal Express or a similar delivery service provider, if possible.

⁷ The Commission's procedures concerning public disclosure and confidential treatment can be found at 15 U.S.C. Sections 46(f) and 57b-2, and Commission Rules 4.10-4.11 (16 C.F.R. Sections 4.10-4.11 (1984)).

⁸ Failure to retain any documents that may be relevant to this matter may result in civil or criminal liability.

Thank you for your prompt attention to this matter. Please call me at 202-326-3377 or Molly Crawford at 202-326-3076 if you have any questions about this request or need any additional information.

Sincerely,

/s/ Lisa W. Schifferle

Lisa W. Schifferle
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission

EXHIBIT 2

DECLARATION OF DOUGLAS H. MEAL, ESQ.

1. I am an attorney at Ropes & Gray LLP and counsel to Wyndham Worldwide Corporation (“WWC”) and Wyndham Hotels and Resorts, LLC (“WHR”). I have been outside counsel to WHR throughout the course of the Federal Trade Commission (“FTC”) investigation that is the subject of the petition to quash to which this declaration is attached (“Petition to Quash”). I make this declaration in support of that petition. I have personal knowledge of the matters set forth in this declaration.

2. I am over 18 years old and competent to make this Declaration.

3. I have read thoroughly, and have personal knowledge of the matters set forth in, the “Background” section of the Petition to Quash. Each of the factual statements made in that “Background” section is accurate to the best of my knowledge, information, and belief.

4. In April 2010, the FTC sent a voluntary access letter (the “Access Letter”) to WHR in connection with this investigation. The letter sought responses to written questions and the production of documents from WHR.

5. The FTC sent written and email communications posing questions supplemental to those contained in the Access Letter on August 13, 2010, August 27, 2010, and April 12, 2011. Additional oral requests for supplemental information and/or documents were made by the FTC during the Staff’s May 12, 2011 and December 15, 2011 meetings with WHR.

6. Exhibit A hereto lists each and every information request made of WHR by the FTC during the investigation prior to the issuance of the civil investigative demand (“CID”) that

is the subject of the Petition to Quash and the manner through which WHR responded to that request.

7. In response to the 29 FTC requests that implicated documents, WHR provided over 1,010,000 pages of electronic and paper documents.

8. In response to the 51 FTC requests that required a narrative response, WHR provided written narratives on July 19, 2010, September 8, 2010, September 14, 2010, October 18, 2010, and January 10, 2011. The narrative responses total 72 pages in length, single spaced.

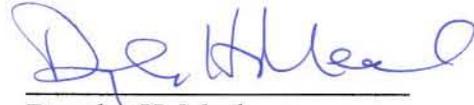
9. WHR participated in 7 in-person meetings with the FTC for the purpose of addressing information requests made by the FTC and, over the course of these meetings, presented responses to 29 FTC requests. Exhibit B hereto lists the dates and topics covered by WHR's presentations to the FTC.

10. Exhibit C hereto lists each and every interrogatory contained in the CID in the column marked "Interrogatory". The column marked "Prior Request" notes any previous FTC request that, in whole or in part, sought the same information as the corresponding interrogatory seeks. In total, 42 of the 89 interrogatories contained in the CID pose questions to which WHR has at least partially responded previously.

11. Exhibit D hereto lists each and every document request contained in the CID in the column marked "Document Requests". The column marked "Prior Request" notes any previous FTC request that, in whole or in part, sought the same documents as the corresponding document request seeks. In total, 25 of the 38 document requests contained in the CID pose questions to which WHR has at least partially responded previously.

I declare under penalty of perjury that the foregoing is true and accurate.

Executed: January 20, 2012



Douglas H. Meal

EXHIBIT 2A

DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
Identify the complete legal name of Wyndham and all other names under which it does, or has done, business, its corporate mailing address, and the date and state of incorporation.	Access Letter Q1	Narrative
Identify and describe Wyndham's parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchisees, operations under assumed names, and entities over which it exercises supervision or control. For each such entity, describe in detail the nature of its relationship to Wyndham and provide copies of any contracts regarding its relationship with Wyndham.	Access Letter Q2	Narrative
Provide documents sufficient to identify and describe in detail Wyndham's business. The response should include but not be limited to: the products and services Wyndham (including but not limited to hotels managed by franchisees that use the Wyndham trade name) offers, sells, or otherwise provides to customers;	Access Letter Q3a	Narrative
information identifying, annually, total revenue and total number of employees.	Access Letter Q3b	Narrative
Identify the name, location, and operating system of each computer network WHR (including but not limited to its franchisees or other related entities) used to store, maintain, process, transmit, handle, or otherwise use (collectively hereinafter, "store and process") personal information (such as to prepare, send, and receive authorization requests for credit and debit card transactions) as of January 1, 2008.	Access Letter Q4	Narrative; Documents
For each network identified in the response to Request 4, above: identify the type(s) of personal information stored and processed on the network, the source of each type of information (including, but not limited to: credit or debit cards; information provided by customers to obtain gifts or rewards; and information provided by third parties); and describe in detail how each type of information is stored and processed by Wyndham;	Access Letter Q5a	Narrative; Documents
provide: blueprints and diagrams setting out in detail the components, topology, and architecture of the network. Responsive documents should include, but not be limited to: documents that identify and locate the components of the network, such as computers; POS devices; cash registers; remote access equipment (such as wireless access points); servers; firewalls; routers; internet, private line, and other connections; connections to other Wyndham networks and outside networks; and security mechanisms and devices (such as intrusion detection systems);	Access Letter Q5b1	Documents
a narrative that describes in detail the components of the network and explains the functions of the components, and how the components operate together on the network;	Access Letter Q5b2	Narrative

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS**

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
provide documents setting out, and describe in detail, the security procedures, practices, policies, and defense(s) (such as access controls or encryption) in place to protect personal information from unauthorized access while stored on the network, transmitted within the network or between networks, and/or processed on the network;	Access Letter Q5b	Documents
provide the name(s), title(s), and contact information of the individual(s) responsible for creating, designing, managing, securing, and updating the network. The responses to each subpart of this Request should describe in detail each material change or update that has been made that concerns, refers, or relates to the subpart, as well as the date the change or update was implemented and the reason(s) for the change or update. If each network has the same standard framework, then you may provide one example rather than providing repeated copies of the same standard network.	Access Letter Q5e	Documents
Describe in detail, and provide documents setting out, the process(es) Wyndham (including but not limited to its franchisees or any other related entities outlined in response to Request #2) uses to provide authorization for credit or debit card transactions ("card authorization"). The response should: set forth the complete transmission or flow path for authorization requests and responses and the underlying information for each network involved in any way in card authorization, starting with the entity to whom a card is presented to pay for a purchase and including each intermediary on the path (including, but not limited to Visa, MasterCard, American Express, Discover [hereinafter collectively, "bank associations"]; acquiring, issuing, and other banks; Wyndham; third-party processors; merchant servicers; independent sales organizations; and other entities) and final destination, and ending with receiving the response to the authorization request;	Access Letter Q6 a	Documents
identify each portion of the transmission or flow paths set out in the response to Request 6(a), above, where authorization requests, authorization responses, or the underlying personal information are transmitted in clear text, if any, as well as the time period during which the requests, responses and information were transmitted in clear text;	Access Letter Q6 b	Documents
identify the system(s), computer(s), or server(s) used to aggregate authorization requests in whole or in part and transmit them to bank associations and banks ("card authorization server"), and, for each server, identify the application(s) used for card authorization and the services enabled on the server, and describe in detail how the server has been protected from unauthorized access (such as protected by its own firewall);	Access Letter Q6 c	Documents

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS**

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
describe in detail how and where authorization requests and responses and underlying personal information are stored or maintained (such as by being stored on a card authorization server or written to transaction logs located elsewhere on a network), as well as how stored or maintained requests, responses, and information have been protected from unauthorized access;	Access Letter Q6 c	Documents
identify and describe the number of authorization requests and responses that Wyndham received, forwarded, processed, stored, or transmitted for each month over the period in question, as well as the type of card presented to the merchant (such as credit or debit) and the disposition of the request (such as approved, declined, not completed, not authorized, or other classification, description, or category).	Access Letter Q6 e	Documents
For each breach, describe in detail and produce documents sufficient to identify how and when Wyndham first learned about the breach.	Access Letter Q7	Narrative; Documents
Provide all documents prepared by or for Wyndham that identify, describe, investigate, evaluate, or assess: (a) how each breach occurred; (b) the time period over which it occurred; (c) where each breach began (e.g., what the point of entry was and where it was located on the network); and (d) the path the intruder followed from the point of entry to the information compromised and then in exporting or downloading the information (including all intermediate steps). Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in each breach; reports of penetration and gap analysis; logs that record the intruder's steps in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was configured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of each breach prepared internally and by third-parties; and other records relating or referring to each breach, including minutes or notes of meetings attended by Wyndham's personnel and documents that identify the attacker(s).	Access Letter Q8	Documents

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS**

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
Identify the name and location of each computer network on which personal information may have been accessed as a result of each breach, and for each such network describe in detail and provide all documents that relate to: the type(s) (e.g., consumer's name, address, and payment card number, expiration date, and security code) and amount(s) of personal information that was or may have been obtained, including but not limited to the number of credit and/or debit card numbers;	Access Letter Q9a	Narrative; Documents
any subsequent unauthorized use of credit and/or debit cards alleged in any way to be linked to each instance of unauthorized access, including, but not limited to, the number of instances where credit and/or debit cards were used without the card holder's authorization, the dates of such use, and the amounts charged or debited. Responsive documents should include, but not be limited to: fraud reports, alerts, or warnings issued by bank associations, banks, or other entities; lists identifying credit, debit, and other types of cards that have been used without authorization or may have been exposed by each breach as well as the issuing banks; documents that assess, identify, evaluate, estimate, or predict the amount of fraudulent purchases resulting from each breach; claims made against Wyndham's acquiring bank(s) under bank network alternative dispute resolution programs (e.g., pre-compliance and compliance actions), and the resolution of any such claims; claims made against Wyndham by banks that issued cards that have been used for unauthorized purchases (such as by demand letters); claims of fraud and/or identity theft, including, but not limited to, affidavits filed by consumers with their banks; and documents that assess, identify, evaluate, estimate, or predict the number of credit, debit, and other types of cards that have been cancelled and/or reissued, the cost per card and in total of cancelling and/or reissuing cards, and additional costs to Wyndham and/or third parties, attributable to each breach (such as for increased monitoring for fraud or providing fraud insurance to consumers affected by each breach);	Access Letter Q9b	Narrative; Documents
the security procedures, practices, policies, and defenses in place when the first instance of each breach occurred as well as any changes to those security procedures, practices, policies, or defenses made thereafter;	Access Letter Q9c	Narrative; Documents
each action Wyndham has taken in response to learning about the unauthorized access to personal information (e.g., notifying consumers or law enforcement, improving security), including when the action was taken; and	Access Letter Q9d	Narrative; Documents
investigations of or complaints filed with or against Wyndham that concern unauthorized access to personal information, including but not limited to correspondence with Wyndham and documents filed with: Federal, State, or local government agencies; Federal or State courts; and Better Business Bureaus.	Access Letter Q9e	Narrative; Documents

DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
According to news articles, at least one breach involved a hacker accessing a Wyndham data center through a franchisee. Identify which franchisees, subsidiaries, or data centers were involved in each of the three breaches.	Access Letter Q10a	Documents
For each such franchisee, subsidiary or data center identified in response to Request 10a, describe and provide documents relating to Wyndham's requirements regarding such entity's compliance with Wyndham's security practices.	Access Letter Q10b	Narrative; Documents
For each such franchisee, subsidiary or data center identified in response to Request 10a, describe and provide documents relating to the network relationship between the entity and Wyndham, including but not limited to: who supplies such entity with its networks and/or who owns the networks; who maintains those networks; who sets security standards for those networks; who monitors those networks; who is responsible for security on those networks; and who is authorized to have access to those networks.	Access Letter Q10c	Narrative; Documents
According to a statement by Wyndham, at least one breach may have affected consumers in countries outside of the United States. Describe in detail and provide documents sufficient to identify whether non U.S. consumers' personal information was or may have been obtained and, if so, the types and amounts of information that was or may have been obtained; the country where the information was originally collected; and whether the information was originally collected by, came from, or was sent to an entity in a member country of the European Union.	Access Letter Q11a	Narrative
State whether Wyndham is a certified Safe Harbor company and, if so, identify the date of certification and provide all documents and information used by Wyndham as part of its application for certification under the program.	Access Letter Q11b	Narrative
Provide documents sufficient to identify, and describe in detail: all networks located outside of the United States used by Wyndham to store and process personal information; the physical location(s) of each network; and the function(s) and business purpose(s) of each network.	Access Letter Q11c	Narrative
For each system identified in response to Request 11(c), above, describe in detail the extent and nature of any interconnection or interface with Wyndham networks located in the United States.	Access Letter Q11d	Narrative
For each of the three breaches, identify how (such as by public announcement or individual breach notification letter), when, how many, and by whom customers were notified that their information was or may have been obtained without authorization. If notification has been made, explain why notification was made (e.g., compelled by law) and provide a copy of each substantively different notification. If notification was not provided as soon as Wyndham became aware of each breach or was not provided to all affected customers or at all, explain why not.	Access Letter Q12	Narrative; Documents

DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
Describe and provide copies of each different policy adopted and statement made by Wyndham to consumers regarding the collection, disclosure, use, and protection of their personal information or customer information, including any policies and statements relating to the privacy or security of such information, and for each policy or statement, identify the date(s) when it was adopted or made, and describe all means by which it was distributed.	Access Letter Q13	Narrative; Documents
Describe in detail and provide documents sufficient to identify any other instances (besides the three breaches) of unauthorized access to Wyndham's computer system of which you are aware, as well as the types of information accessed without authorization and when the unauthorized access occurred.	Access Letter Q14	Narrative
Where does Wyndham Management ("WHM") fit within the organization chart provided?	8/13/2010 Letter Q1	Narrative
Who did Pete Gibson report to after March 2009 when the WHG CIO position was eliminated? Who does the head of WHG IT report to today?	8/13/2010 Letter Q2	Narrative
Who did Jim Copenheaver (and any successor) report to after March 2009 when the WHG CIO position was eliminated?	8/13/2010 Letter Q3	Narrative
[T]he names and titles of key Wyndham employees who had line responsibilities over various areas of data security for Wyndham Worldwide Corporation ("Wyndham") and its various subsidiaries during the time periods relevant to each of the security breaches. The individuals whose identities, titles, and Wyndham affiliations we sought were Wyndham employees who: served as liaison(s) to Trustwave concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
served as liaison(s) to Fishnet concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
served as data security liaison(s) with the Wyndham franchisees, and with WHM (if different), concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
served as liaison(s) to Micros/FideliolProtobase concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
served as liaison(s) to American Express concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative

DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
served as liaison(s) to the other card brands concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
served as liaison(s) with state law enforcement concerning the subject breaches;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
were in charge of risk assessment for data security;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
were in charge of electronic security;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
were in charge of breach detection;	8/13/2010 Letter Key Wyndham Employees Question	Narrative
were in charge of developing a breach response plan; and	8/13/2010 Letter Key Wyndham Employees Question	Narrative
were in charge of developing breach response protocols.	8/13/2010 Letter Key Wyndham Employees Question	Narrative
[Whether] Wyndham formed any ad hoc executive committees tasked with responsibilities for evaluating any breach-related issues. If so, we sought to learn how many such committees were established since this date, and the dates they were established. For each committee, we sought to learn who the members of each committee were, and what were their titles and responsibilities on each such committee.	8/13/2010 letter Wyndham Exec and Board Reactions Q1	Narrative

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS**

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
[Whether] any Wyndham Board formed any Board committees tasked with any responsibilities for evaluating any breach-related issues. If so, we sought to learn how many such committees were established since this date, and the dates they were established. For each committee, we sought to learn who the members of each committee were, and what were their titles and responsibilities on each such committee.	8/13/2010 letter Wyndham Exec and Board Reactions Q2	Narrative
[Whether] any members of any of the Wyndham Boards were provided with documents that discussed any of the data security breaches. If so, we sought to learn who had received such documents, and on which dates they were given such documents.	8/13/2010 letter Wyndham Exec and Board Reactions Q3	Narrative
[T]he identities of each member of each "action" team Wyndham assembled to respond to each of the breaches, and a description of their responsibilities.	8/13/2010 letter Wyndham Breach Teams Question	Narrative
[W]hether Wyndham had retained the electronic files of key individuals such as Jim Copenheaver, Pete Gibson, and Jeff Edwards who have since left the company.	8/13/2010 letter Misc. Question	Narrative
The names, titles, and Wyndham affiliations of the employees who: "were responsible for evaluating the impact, if any, that each breach had on Wyndham's sales, including but not limited to form of payment used, or decision to purchase lodgings or services from another hotel brand"	8/27/2010 Email Q1	Narrative
The names, titles, and Wyndham affiliations of the employees who: "served as liaison(s) to any third party Qualified Security Assessor and/or to any third parties that prepared PCI Reports on Compliance"	8/27/2010 Email Q2	Narrative
The names, titles, and Wyndham affiliations of the employees who: "were interviewed in connection with preparing any PCI Report on Compliance"	8/27/2010 Email Q3	Narrative
The names, titles, and Wyndham affiliations of the employees who: "were in charge of any PCI self-certification process that used a Self-Assessment Questionnaire"	8/27/2010 Email Q4	Narrative
The names, titles, and Wyndham affiliations of the employees who: "held the responsibility of Security Event Information Manager"	8/27/2010 Email Q5	Narrative
The names, titles, and Wyndham affiliations of the employees who: "were in charge of developing information security policies, procedures, and/or standards for Wyndham and, if applicable, its franchisees"	8/27/2010 Email Q6	Narrative
The names, titles, and Wyndham affiliations of the employees who: "were members of the assurance team put in place to monitor and escalate any critical security alerts, as referenced on page 33 of your July 19,2010 letter response."	8/27/2010 Email Q7	Narrative
Last known contact information for each former employee named in WHR's responses to your August 13,2010 letter and the August 27 Request.	8/27/2010 Email Misc	Narrative

DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
The August 27 Request also referred back to Request 14 of the Access Letter, which asked for information regarding instances other than the three breaches where personal information was accessed without authorization by means of an intrusion into "Wyndham's" computer system. In the August 27 Request you asked that WHR's response to Request 14 be extended not only to WHR itself, but also to "any WHR parent, subsidiary, division, affiliate or franchisee ." WHR is unaware of any other instance where unauthorized access to personal information occurred as a result of an intrusion into the computer system of any entity that was then a WHR parent, subsidiary, division, affiliate, or franchisee.	8/27/2010 Email Misc	Narrative
WWC's role in information security for WHG/WHR and how that role changed during the applicable time period.	4/12/2011 Email	Presentation
What information security policies, procedures, and practices (both technological and administrative) were in effect at WHG and WHR at the time of the breaches? (for example, we have the WWC Enterprise Information Security Policy and Compliance Program from 12/08 and we do not know if this was applicable to WHR and WHG, or if they followed something different).	4/12/2011 Email	Presentation; Documents
What, if any, penetration testing and vulnerability assessments were being conducted during the time of the breaches, including at the franchise level?	4/12/2011 Email	Presentation
The architectural changes that were made after the second breach so that we can better understand how the system looked at the time of the first two breaches and what changed.	4/12/2011 Email	Presentation
How Wyndham's support role for franchisees changed, if at all, following a franchisee's signing of the technology addendum.	4/12/2011 Email	Presentation
With respect to each breach, how the breaches were detected, including why, in certain instances, they were not caught earlier (e.g. we understand from the forensic report that there were many account lockouts prior to the first breach that seemed not to have triggered an investigation), as well as remediation efforts following each of the breaches.	4/12/2011 Email	Presentation
The vulnerabilities found in the forensic reports that led to the three breaches, including, for example, insufficient logging; weak passwords; and weak infrastructure and design.	4/12/2011 Email	Presentation
Estimates of harm resulting from each breach. Updated information on 1) how much in fines Wyndham and its franchisees have been assessed as a result of each of the breaches, including what is still being appealed; and 2) how much in fraudulent purchases the card brands have alleged resulted from the breaches.	4/12/2011 Email	Presentation
Policies re Quality Assurance	4/12/2011 Email	Presentation
When did the WWC Information Security Policy (Tab 2) first become effective and, to the extent it was not in effect as of January 2008, what preceded it at WHG and WHR?	Follow-up from 5/12/2011 Meeting	Presentation

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS**

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
Please provide any prior versions of the WWC Information Security Policy (Tab 2) that were in effect from January 1, 2008 forward.	Follow-up from 5/12/2011 Meeting	Documents
How are policies such as the WWC Information Security Policy disseminated by WWC and how if at all has that dissemination process changed since January 1, 2008?	Follow-up from 5/12/2011 Meeting	Presentation
How many people in WWC's information security function currently have direct responsibility for information security at WHR; how has that number changed during the period that WWC has been responsible for information security at WHR; and during the period after January 1, 2008 when WHG was responsible for information security at WHR, how many people in WHG's information security function had direct responsibility for information security at WHR?	Follow-up from 5/12/2011 Meeting	Presentation
The Huron Report states that WWC did an internal information security audit (see FTC2 998601). Is that correct and, if so, please either identify or provide a copy of that audit.	Follow-up from 5/12/2011 Meeting	Documents
Please confirm that the CIRT process and procedures were in effect from January 1, 2008 forward as they appear at Tab 3 or, if they were not, please identify or provide any different version of these procedures that was in effect at any time after January 1, 2008.	Follow-up from 5/12/2011 Meeting	Presentation; Documents
Please state when the "Property Technology Standards and Procedures" (FTC2 836624) came into effect and, to the extent those standards and procedures were not in effect from January 1, 2008 forward, identify any prior version of those standards and procedures or any other such standards and procedures that were in effect during that period.	Follow-up from 5/12/2011 Meeting	Presentation; Documents
Page 16 of WHR's letter to the FTC dated July 19, 2010 states that WHR's IT function "customarily manages the PMS environment on behalf of each Wyndham-branded hotel." Please state whether that was the case throughout the period of January 1, 2008 forward and, if it was not, please state when WHR's IT function commenced managing the PMS environment on behalf of each Wyndham-branded hotel and state what entity managed the Wyndham-branded hotels PMS environments prior to WHR'S IT function taking on that responsibility.	Follow-up from 5/12/2011 Meeting	Presentation
In reference to the bullet points in the top half of page 33 of WHR's letter to the FTC dated July 19, 2010, please provide the details of the new security infrastructure that was built;	Follow-up from 5/12/2011 Meeting QA-1	Presentation
please explain how WHR's Global Threat Management Systems was "expanded" to include critical hotel property systems;	Follow-up from 5/12/2011 Meeting QA-2	Presentation
please explain how the remote access process changed;	Follow-up from 5/12/2011 Meeting QA-3	Presentation

DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
please identify what process improvements were made for account administrative authorization; and	Follow-up from 5/12/2011 Meeting QA-4	Presentation
please describe the holistic view of the WHR environment that was created.	Follow-up from 5/12/2011 Meeting QA-5	Presentation

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT A
REQUESTS CONTAINED IN ACCESS LETTER AND SUPPLEMENTAL COMMUNICATIONS**

<u>FTC Narrative Question</u>	<u>Question Source</u>	<u>Type of Response</u>
In reference to the bullet points on the bottom half of page 33 of the WHR's letter to the FTC dated July 19, 2010, please describe whether and if so to what extent, the following items were in place for the WHR network during the period from January 1, 2008 to the end of 2009: log monitoring;	Follow-up from 5/12/2011 Meeting QB-1	Presentation
intrusion prevention and/or intrusion detection systems;	Follow-up from 5/12/2011 Meeting QB-2	Presentation
file integrity monitoring;	Follow-up from 5/12/2011 Meeting QB-3	Presentation
antivirus software; and	Follow-up from 5/12/2011 Meeting QB-4	Presentation
firewalls and content filtering to block connectivity with known bad IP addresses.	Follow-up from 5/12/2011 Meeting QB-5	Presentation
Prior to the tech addenda that were entered into by the franchisees in 2009, were there any specific requirements imposed on WHR franchisees by WHR from an information security perspective (and if so what were those requirements) and	Follow-up from 5/12/2011 Meeting QC-a	Presentation
what if any information security services did WHR provide for WHR franchisees.	Follow-up from 5/12/2011 Meeting QC-b	Presentation
In regard to the account lockouts that are referenced in the Fishnet forensic report and that were discussed during WHR's presentation on May 12, 2011, please identify or provide a copy of the account lockout report referenced in the Fishnet forensic report.	Follow-up from 5/12/2011 Meeting QD	Documents
Page 10 of WHR's letter to the FTC dated July 19, 2010 states that "at all times herein, WHR's computer network, including the cardholder data portion of that network, has been, and remains, logically separated from the WHG computer network." Please provide a detailed description of how that logical separation was implemented during the time period from January 1, 2008 forward and continues to be implemented today.	Follow-up from 5/12/2011 Meeting QE	Presentation
Please provide details on Wyndham's quality assurance process.	Follow-up from 12/15/2011 Meeting	Presentation; Documents

EXHIBIT 2B

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT B
WHR PRESENTATIONS TO FTC IN RESPONSE TO ACCESS LETTER**

No.	Presentation Date	Topic(s)
1	11/10/2010	Presentation regarding various topics of FTC interest, including: <ul style="list-style-type: none"> - Background information on WHR - How WHR responded to the Intrusions - WHR's extensive efforts to notify consumers
2	3/14/2011	Presentation regarding relationship between WHR and its franchisees.
3	4/5/2011	Presentation regarding information security services currently provided by WHR to franchisees.
4	5/12/2011	Presentation regarding information security services currently provided by WHR to franchisees.
5	5/26/2011	Presentation on various questions raised by Staff following 5/12 Meeting, including: <ul style="list-style-type: none"> - History and dissemination of WWC Information Security Policy - Structure of WHR IT/IS functions within WWC and WHG - 2007 GCC Audit - Incident response procedures - Property Technology Standards and Procedures document - WHR IT's role in managing PMS environment on behalf of Wyndham-branded hotels - improvements made to network following second breach - security measures in place on WHR network at various periods of time - Information Security requirements imposed on franchisees and services provided to franchisees. - Account lockout report related to first intrusion - Logical separation of WHR cardholder data environment
6	7/7/2011	Presentation regarding various topics of FTC interest, including: <ul style="list-style-type: none"> - Representations made by WHR to its customers regarding data security - The relationship between WHR and WHG, including the relationship between their networks - Inclusion of employees within the definition of consumer
7	12/20/2011	Presentation regarding the quality assurance process used by Wyndham to ensure compliance by the Wyndham-branded hotels with their contractual obligations, including the Brand Standards.

EXHIBIT 2C

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

<u>No.</u>	<u>Interrogatory</u>	<u>Prior Request</u>
1	Identify each Wyndham entity's total number of employees and total annual revenues; each Wyndham-franchised hotel, its mailing address, the date on which it first entered into a franchise agreement with Wyndham Hotels, and, if applicable, the date on which its franchise agreement was terminated; and each Wyndham-managed hotel, its mailing address, the date on which it first entered into a management agreement with Hotel Management, and, if applicable, the date on which its management agreement was terminated.	Access Letter Q3b
2	Provide a high-level diagram (or diagrams) that sets out the components of each computer network used by Wyndham Hotels and Hotel Management to store and process personal information, including any network hosted by Wyndham Hotels or Hotel Management on behalf of any Wyndham-branded hotel, and any network that would allow access to the network(s) of any Wyndham-branded hotel that stores and processes personal information. To the extent your network(s) changed throughout the applicable time period, you should provide separate diagrams for the time periods immediately preceding each data breach identified in response to Interrogatory Specification 16. In addition, provide a narrative that describes the components in detail and explains their functions and how they operate. Such diagram(s) and description shall include the location (within the network) of: computers; servers; firewalls; routers; internet, private line, and other connections; connections to other internal and external networks; virtual private networks; remote access equipment (such as wireless access points); websites; and security mechanisms and devices (such as intrusion detection systems)	Access Letter Q4; Access Letter Q5a; Access Letter Q5b
3	Describe in detail how the Wyndham-branded hotels' networks are connected to any Company network(s), including all connections between the Company's central reservation system(s), its guest loyalty database(s), and the Wyndham-branded hotels. Your response should explain whether and how the Wyndham-branded hotels may access the central reservation system(s) or guest loyalty database(s), describe the personal information contained in each, and describe any access controls in place to limit access to the central reservation system or guest loyalty database.	

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

4a	Describe the process(es) used by Wyndham Hotels and Hotel Management, on behalf of themselves or any Wyndham-branded hotel, to obtain authorization for payment card transactions (“card authorization”). This description should include: the complete transmission or flow path for authorization requests and responses and the underlying information for each network involved in card authorization, starting with the merchant to whom a card is presented to pay for a purchase and including each intermediary on the path (including, but not limited to: bank associations; acquiring, issuing, and other banks; Wyndham Hotels or Hotel Management; third-party processors; merchant servicers; independent sales organizations; and other entities), and ending with receiving the response to the authorization request;	Access Letter Q6a
4b	each portion, if any, of the transmission or flow paths described in response to Interrogatory Specification 4a, above, where authorization requests, authorization responses, or the underlying personal information were transmitted in clear text, as well as the time period during which the requests, responses, and information were transmitted in clear text;	Access Letter Q6b
4c	identification of the system(s), computer(s), or server(s) used to aggregate authorization requests in whole or in part and transmit them to bank associations and banks (“card authorization server”), and, for each server, the application(s) used for card authorization and the services enabled on the server, and a description of how the server has been protected from unauthorized access (such as protected by its own firewall); and	Access Letter Q6c
4d	where authorization requests and responses and underlying personal information are stored or maintained (such as by being stored on a card authorization server or written to transaction logs located elsewhere on a network), as well as how stored or maintained requests, responses, and information have been protected from unauthorized access and the length of time they are retained.	Access Letter Q6d
5a	Describe in detail Wyndham Worldwide’s role in the Information Security Programs of The Hotel Group, Wyndham Hotels, Hotel Management, the Wyndham-franchised hotels, and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following: a. Wyndham Worldwide’s role in developing and implementing each entity’s Information Security Program;	4/12/2011 Email
5b	the training Wyndham Worldwide provides to each entity related to the protection of personal information, including PCI DSS compliance;	
5c	all policies, practices, and procedures relating to Wyndham Worldwide’s audits, assessments, and oversight of each entity’s Information Security Program, including any role it has had in ensuring each entity’s compliance with PCI DSS;	

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

5d	Wyndham Worldwide's role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;	4/12/2011 Email; Follow-up from 12/15/2011 Meeting
5e	Wyndham Worldwide's role in providing payment card authorization for each entity; and	Access Letter Q6a
5f	the Wyndham Worldwide employee(s) responsible for overseeing each entity's Information Security Program.	Access Letter Q5e
6a	Describe in detail The Hotel Group's role in the Information Security Programs of Wyndham Hotels, Hotel Management, the Wyndham-franchised hotels and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following: a. The Hotel Group's role in developing and implementing each entity's Information Security Program;	4/12/2011 Email
6b	the training The Hotel Group provides to each entity related to the protection of personal information, including PCI DSS compliance;	
6c	all policies, practices, and procedures relating to The Hotel Group's audits, assessments, and oversight of each entity's Information Security Program, including any role it has had in ensuring each entity's compliance with PCI DSS;	
6d	The Hotel Group's role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;	Follow-up to 12/15/2011 Meeting
6e	The Hold Group's role in providing payment card authorization for each entity; and	Access Letter Q6a
6f	The Hotel Group employee(s) responsible for overseeing each entity's Information Security Program.	
7a	Describe in detail Wyndham Hotels' role in the Information Security Programs of Hotel Management, the Wyndham-franchised hotels, and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following: a. Wyndham Hotels' role in developing and implementing each entity's Information Security Program;	Discussed at 4/5/2011 Meeting
7b	the training Wyndham Hotels provides to each entity related to the protection of personal information, including PCI DSS compliance;	Discussed at 4/5/2011 Meeting
7c	all policies, practices, and procedures relating to Wyndham Hotels' audits, assessments, and oversight of each entity's Information Security Program, including any role it has had in ensuring each entity's compliance with PCI DSS;	Discussed at 4/5/2011 Meeting

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

7d	Wyndham Hotels' role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;	Discussed at 4/5/2011 Meeting
7e	Wyndham Hotels' role in providing payment card authorization for each entity; and	Access Letter Q6
7f	the Wyndham Hotels employee(s) responsible for overseeing each entity's Information Security Program, his title(s), and the total number of employees responsible for handling information security.	8/13/2010 letter Key Wyndham Employees Question
8a	Identify and describe in detail Hotel Management's role in the Information Security Program of the Wyndham-franchised hotels and the Wyndham-managed hotels, including a description of how its role has changed throughout the applicable time period. Your response should include, but not be limited to, a description of the following: a. Hotel Management's role in developing and implementing each hotel's Information Security Program;	
8b	the training Hotel Management provides to each hotel related to the protection of personal information, including PCI DSS compliance;	
8c	all policies, practices, and procedures relating to Hotel Management's audits, assessments, and oversight of each hotel's Information Security Program, including any role it has had in ensuring each hotel's compliance with PCI DSS;	
8d	Hotel Management's role in developing and implementing any program to ensure the compliance of the Wyndham-franchised hotels and the Wyndham-managed hotels with any Company operating standards or system standards;	
8e	Hotel Management's role in providing payment card authorization for each hotel; and	
8f	a list of all Hotel Management employee(s) responsible for overseeing each hotel's Information Security Program.	
9a	Identify and describe in detail the 2009 decision that Wyndham Worldwide would assume responsibility from The Hotel Group for Wyndham Hotels' Information Security Program, as described in the Access Letter Response (the "decision"). Your answer should include, but not be limited to, the following: a. which Company personnel were involved in the decision making process;	
9b	who approved the decision;	
9c	all reasons for the decision; and	
9d	any personnel changes as a result of the decision, including any transfer of personnel employed by one Wyndham entity to another Wyndham entity as a result of the change.	

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

10a	10. Describe in detail the role of each Wyndham entity in managing the property management systems and payment processing applications of the Wyndham-branded hotels, including when and how those roles changed throughout the applicable time period and how those roles differed between the Wyndham-franchised hotels and the Wyndham-managed hotels. Your answer should include, but not be limited to, a description of the following (separately for each Wyndham entity): a. the types of property management systems and payment processing applications used by the Wyndham-branded hotels (including, but not limited to, Opera, Fidelio, and ProtoBase);	Follow-up from 5/12/2011 Meeting
10b	the guidance provided to the Wyndham-branded hotels regarding the types of hardware and software required for their property management systems or payment processing applications, including any needed upgrades;	Follow-up from 5/12/2011 Meeting
10c	the support provided to the Wyndham-branded hotels in configuring their property management systems or payment processing applications;	Follow-up from 5/12/2011 Meeting
10d	the oversight provided of Micros and Southern DataComm in installing and configuring the Wyndham-branded hotels' property management systems or payment processing applications;	
10e	the extent to which any Wyndham entity put any property management system or payment processing application, including Protobase, into debugging mode or was aware that such systems were running in debugging mode; and	
10f	any other services performed in each Wyndham entity's management of the Wyndham-branded hotels' property management systems or payment processing applications.	Follow-up from 5/12/2011 Meeting
11	Identify any Wyndham-branded hotels that failed to sign the Technology Addendum to their franchise or management agreement in 2009, as described in the Access Letter Response, and state (1) if given, the reason provided by the hotel for not signing the Technology Addendum; (2) whether the franchise or management agreement with the hotel was terminated; (3) the date of such termination; and (4) whether a hotel's failure to sign the Technology Addendum resulted in any other consequences and, if so, state what the consequences were.	
12a	Separately for each Wyndham entity and for the Wyndham-branded hotels, provide the following information (including any changes that occurred throughout the applicable time period): a. all practices to control, monitor, and record authorized and unauthorized access to personal information on its network(s);	
12b	the frequency and extent to which network users receive information security training or security awareness materials;	
12c	whether and, if so, when risk assessment(s) were performed to identify risks to the security, integrity, and confidentiality of personal information on its network(s);	

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

12d	the manner in which it or another person or entity tests, monitors, or evaluates the effectiveness of its Information Security Program, including practices to ensure that all persons or entities that obtain access to personal information are authorized to do so and use the information for only authorized purposes.	
12e	when testing, monitoring, or evaluation activities were conducted and all changes made to security practices on the network(s) based upon such testing, monitoring, or evaluation;	
12f	all other security procedures, practices, policies, and defense(s) (such as access controls or encryption) in place to protect personal information from unauthorized access while stored on the network, transmitted within the network or between networks, or processed on the network, including the date on which it was implemented; and	
12g	identify the employee(s) responsible for implementing its Information Security Program.	
13a	For each risk assessment identified in response to Interrogatory Specification 12c, as well as any assessment(s) performed by Fishnet Security, Inc. beginning in 2005 of Wyndham Hotels' computer network(s) or Information Security Program, identify: a. the date of the assessment and the name and title of the person(s) responsible for conducting and overseeing the assessment;	
13b	the steps taken in conducting the assessment;	
13c	the specific risks identified in the assessment; and	
13d	how and by whom each risk was addressed.	
14a	For each Wyndham Hotels and Hotel Management Service Provider: a. identify the Service Provider;	
14b	identify the types of personal information that Wyndham Hotels and Hotel Management allow the Service Provider to access;	
14c	describe the manner and form of access (such as physical access to Company offices or remote access to computer systems, including administrative access);	
14d	state the purpose(s) for such access; and	
14e	describe how the Company monitors the Service Provider to confirm that it has implemented and maintained security safeguards adequate to protect the confidentiality and integrity of personal information.	
15a	Describe in detail the specific technical, administrative, and physical safeguards taken to re-architect and upgrade the Wyndham Hotels' Phoenix Data Center in 2009 as described in the Access Letter Response, including, but not limited to, the following: a. building a new security infrastructure;	Follow-up from 5/12/2011 Meeting
15b	segmenting the Wyndham Hotels' Phoenix data center environment from the Wyndham-branded hotel properties' networks;	Follow-up from 5/12/2011 Meeting
15c	expanding Wyndham Hotels' global threat management system to include critical hotel property systems;	Follow-up from 5/12/2011 Meeting
15d	changing the remote access process;	Follow-up from 5/12/2011 Meeting

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

15e	making process improvements for account administrative authorization;	Follow-up from 5/12/2011 Meeting
15f	ensuring that all internal system administrators now have two-factor authentication for remote access from outside the Wyndham Hotels network;	Follow-up from 5/12/2011 Meeting
15g	creating a holistic view of the Wyndham Hotels' environment; and	Follow-up from 5/12/2011 Meeting
15h	any upgrades made to Wyndham Hotels' virus monitoring.	Follow-up from 5/12/2011 Meeting
16	Identify each data breach that is known to have occurred since January 1, 2008, and, for each data breach identified, describe in detail how, when, and through whom the Company first learned about the breach.	Access Letter Q7
17	Identify all consultants, agents, or other entities that assisted any Wyndham entity in connection with any actions it took relating to the data breaches identified in response to Interrogatory Specification 16. For each such entity, state on which Wyndham entity's behalf the entity was retained and provide a brief description of the services rendered.	
18	Describe in detail any network user account lockouts related to any data breach identified in response to Interrogatory Specification 16, and the Company's investigations of any such lockouts, including but not limited to, when the investigation was initiated, the personnel notified, and the steps taken to determine whether an intruder had gained access to the network(s).	Follow-up from 5/12/2011 Meeting
19a	For each data breach identified in response to Interrogatory Specification 16, identify the name and location of each computer system on which personal information was or may have been accessed as a result of each such breach, and for each such system describe: a. the type(s) and amount(s) of potentially compromised personal information;	Access Letter Q9a
19b	any report of subsequent unauthorized use of compromised personal information alleged in any way to be linked to each instance of unauthorized access, including, but not limited to, the number of instances where payment cards were alleged to have been used without the card holder's authorization, the dates of such use, and the amounts charged or debited;	Access Letter Q9b
19c	each known or suspected intruder;	
19d	the manner by which each intruder obtained access to the compromised personal information, including security practices that permitted or may have permitted the data breach to occur;	4/12/2011 Email
19e	the time period over which: (1) the data breach occurred; and (2) personal information was or may have been accessed;	Provided in response to Access Letter Q9
19f	each security measure implemented in response to the data breach, including the date on which it was implemented; and	Access Letter Q9c

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

19g	sanctions imposed in response to the data breach.	
20a	For each data breach identified in response to Interrogatory Request 16, describe in detail any investigations conducted to determine the likely cause of the breach or the security vulnerabilities that may have led to the breach, including investigations conducted by any Wyndham entity, as well as those conducted on behalf of the Card Associations. Your response should include, but not be limited to, the following: a. a description of the findings of any such investigation;	4/12/2011 Email
20b	a description of any disputes the Company has with the findings of any such investigation;	
20c	a description of the role any Wyndham entity played in overseeing any investigation conducted of a Wyndham-branded hotel; and	
20d	identification of any Company employee(s) responsible for overseeing any such investigations.	
21	For each policy or statement submitted in response to Document Specification 15, identify the date(s) when it was adopted or made, and describe all means by which it was distributed.	Follow-up from 5/12/2011 Meeting
22	Identify all officers and members of the Board of Directors of each Wyndham entity during the applicable time period. In doing so, identify all officers or Board members of any Wyndham entity who are also serving or have ever served as officers or Board members of another Wyndham entity. For each such person, state for which Wyndham entities he or she served as an officer or Board member and the time period during which he or she served in such role.	Information provided in response to 8/13/2010 letter Wyndham Exec and Board Reactions Q3
23	Describe the extent to which accounting, managerial, marketing, distributing, human resources, information security, legal and other functions or facilities are shared or interrelated between each Wyndham entity. Your response should include, but not be limited to, a description of whether any Wyndham entity pays on behalf of any other Wyndham entity (1) its payroll, or (2) the premiums for any director or officer insurance coverage, and whether any Wyndham entity transfers or otherwise allocates for accounting purposes any consideration to another Wyndham entity in exchange for providing any information security-related service.	
24a	24. For any document request specification for which there are documents that would be responsive to this CID, but which were destroyed, mislaid, transferred, deleted, altered, or over-written: a. identify the document;	
24b	state the date such document was destroyed, mislaid, transferred, deleted, altered, or overwritten;	
24c	describe the circumstance under which such document was destroyed, mislaid, transferred, deleted, altered, or overwritten; and	
24d	identify the person authorizing such action.	

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT C
COMPARISON OF ACCESS LETTER REQUESTS TO CID INTERROGATORIES**

25	Identify the person(s) responsible for preparing the response to this CID, and describe in detail the steps taken to respond to this CID, including instructions pertaining to document (written and electronic) and information preservation. Where oral instructions were given, identify the person who gave the instructions and describe the content of the instructions and the person(s) to whom the instructions were given. For each specification, identify the individual(s) who assisted in preparing the response, with a listing of the persons (identified by name and corporate title or job description) whose files were searched by each person.	
26	To the extent that any information provided in the Access Letter Response may require updating or is otherwise incomplete or inaccurate, supplement your response.	Update provided on 1/10/2011

EXHIBIT 2D

DECLARATION OF DOUGLAS H. MEAL EXHIBIT D
COMPARISON OF ACCESS LETTER REQUESTS TO CID DOCUMENT REQUESTS

<u>No.</u>	<u>Interrogatory</u>	<u>Prior Request</u>
1	Each different franchise and management contract with a Wyndham-branded hotel that governs the storing and processing of personal information, including all addenda to such contracts.	
2	All documents provided to Wyndham-branded hotels related to information technology or information security, including but not limited to: training materials; operation manuals; system standards; information security policies; PCI DSS compliance documents; and documents related to property management system or payment application hardware, software, or configuration requirements.	
3	Documents sufficient to describe the relationship between the networks of the Wyndham entities, including but not limited to: who supplies each Wyndham entity with its network(s); who owns the network(s); who maintains the network(s); who sets standards for the network(s); who monitors the network(s); and who is responsible for information security on the network(s).	Access Letter Q4 & Q5
4	Documents sufficient to describe each Wyndham entity's role in managing the Wyndham-branded hotels' computer networks, including but not limited to: who supplies each Wyndham-branded hotel with its network(s); who owns the network(s); who maintains the network(s); who sets standards for the network(s); who monitors the network(s); who is responsible for information security on the network(s); and how the Company's role is different between Wyndham-franchised hotels and Wyndham-managed hotels.	Access Letter 10c
5	Documents sufficient to describe the Company's relationship with any property management system or payment processing vendor, including but not limited to Micros, Southern DataComm, and Elavon, related to the installation, configuration, operation, or technical support of the property management systems or payment processing applications for the Wyndham-branded hotels and Wyndham Hotels' central reservation system. Your response should include, but not be limited to, all contracts between the Company and Micros, Southern DataComm, and Elavon related to property management systems or payment processing applications.	
6	Documents sufficient to describe the Information Security Program of each Wyndham entity, including but not limited to, documents describing:	Access Letter Q9c; 4/12/2011 Email
6a	access controls in place, including who has access to personal information on their network(s), including any Service Providers or Wyndham-branded hotels;	Access Letter Q9c
6b	physical or electronic information security measures taken to protect personal information, including but not limited to practices to monitor and record unauthorized access (such as intrusion detection systems), password requirements, employee turnover procedures, procedures for transporting personal information, and log retention policies;	Access Letter Q9c

DECLARATION OF DOUGLAS H. MEAL EXHIBIT D
COMPARISON OF ACCESS LETTER REQUESTS TO CID DOCUMENT REQUESTS

6c	the means by which each Wyndham entity's computer network(s) may be accessed externally, including by Service Providers or Wyndham-branded hotels;	Access Letter Q5b
6d	the technical configurations of devices and programs it uses to implement its Information Security Program, including but not limited to configurations of firewalls or other means used to control, monitor, or record access to personal information;	Access Letter Q5b; Access Letter Q8
6e	completed or planned testing, monitoring, or evaluation of its Information Security Program; and	Access Letter Q8
6f	information security training provided to network users (such as employees, Wyndham-branded hotels, and Service Providers) regarding the Information Security Program.	Produced in response to Access Letter Q9d
7	All documents that assess, evaluate, question, challenge, or contest the effectiveness of any Wyndham entity's or Wyndham-branded hotel's Information Security Program, or recommend changes to it, including, but not limited to internal and external security assessments, plans, reports, studies, audits, audit trails, evaluations, and tests. Your response should include all documents that relate to each risk assessment described in response to Interrogatory Specification 13, including but not limited to a copy of each internal and external report that verifies, confines, challenges, questions, or otherwise concerns such assessment.	Produced in response to Access Letter Q8
8	For each Service Provider identified in response to Interrogatory Specification 14, all provisions of contracts with the Company relating to the handling of personal information, and all other policies, procedures, or practices that relate to each Service Provider's handling of personal information, including any policies or practices related to granting the Service Provider administrative access to any Company network.	

**DECLARATION OF DOUGLAS H. MEAL EXHIBIT D
COMPARISON OF ACCESS LETTER REQUESTS TO CID DOCUMENT REQUESTS**

9	For each data breach identified in response to Interrogatory Specification 16, all documents prepared by or for the Company that identify, describe, investigate, evaluate, or assess such breach, including but not limited to preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in each breach; reports of penetration and gap analysis; logs that record the intruder's steps in accessing or using compromised personal information; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was configured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, toolkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of each breach prepared internally and by third-parties; and other records relating or referring to each breach, including minutes or notes of meetings attended by the Company's personnel and documents that identify the intruder(s).	Access Letter Q8
10a	All communications between the Company or a Wyndham-branded hotel and Micros, Southern DataComm, or Elavon related to: a. the installation or configuration of any property management system or payment processing application	
10b	any data breach;	Produced in response to Produced in response to Access Letter Q9d
10c	remote access to any network identified in response to Interrogatory Specification 2 or to the network(s) of any Wyndham-branded hotel;	
10d	the use of debugging in any application; and	
10e	the use of passwords, including descriptions of who is responsible for setting passwords and password requirements.	
11a	All communications between the Company and the Wyndham-branded hotels related to: any data breach, and including any documents referencing fines or assessments from any Card Association;	Produced in response to Access Letter Q9 b& d
11b	the use of debugging in any property management system or payment processing application;	
11c	PCI DSS compliance; and	
11d	the use of passwords on any application, including who is responsible for setting passwords and password requirements for accessing the Company's central reservation system or related to the Wyndham-branded hotels' property management systems or payment processing applications.	

DECLARATION OF DOUGLAS H. MEAL EXHIBIT D
COMPARISON OF ACCESS LETTER REQUESTS TO CID DOCUMENT REQUESTS

12	All communications between the Company or a Wyndham-branded hotel and any Card Association related to any data breach identified in response to Interrogatory Specification 16.	Produced in response to Access Letter Q9b & d
13	All communications between the Company or a Wyndham-branded hotel and any consultant, agent, or other entity identified in response to Interrogatory Specification 17 relating to information security or to any data breach.	Produced in response to Access Letter Q9d
14	Documents sufficient to describe the Company's quality assurance program for inspecting the Wyndham-branded hotels' compliance with their franchise or management contracts, including but not limited to, documents that describe:	Follow-up from 12/15/2011 Meeting
14a	how often each Wyndham-branded hotel is inspected;	Follow-up from 12/15/2011 Meeting
14b	which Wyndham entity is responsible for conducting the inspections;	Follow-up from 12/15/2011 Meeting
14c	how the quality assurance program differs between Wyndham-franchised hotels and Wyndham-managed hotels;	Follow-up from 12/15/2011 Meeting
14d	criteria for determining whether and how often to inspect each Wyndham-branded hotel; and	Follow-up from 12/15/2011 Meeting
14e	any inspections done of Wyndham-branded hotels related to either information technology or information security.	Follow-up from 12/15/2011 Meeting
15	All policies, claims, and statements made to consumers by or for the Company regarding the collection, disclosure, use, storage, destruction, and protection of personal information, including any policies, claims, or statements relating to the security of such information.	Access Letter Q13
16	All documents that relate to actual or potential harm to consumers or claims of harm made by consumers that are based on any data breach identified in response to Interrogatory Specification 16. Responsive documents should include, but not be limited to:	4/12/2011 Email
16a	documents that assess, identify, evaluate, estimate, or predict the number of, consumers that have, or are likely to, suffer fraud, identity theft, or other harm; claims made against the Company or any Wyndham-branded hotel for fraud, identity theft, or other harm, such as by affidavits filed by consumers; and documents that assess, identify, evaluate, estimate, or predict the dollar amount of fraud, identity theft, or other costs (such as for increased fraud monitoring or providing fraud insurance) attributable to each such incident; and	
16b	documents that relate to investigations of or complaints filed with or against the Company or any Wyndham-branded hotel relating to each data breach, including, but not limited to, private lawsuits, correspondence with the Company or any Wyndham-branded hotel, and documents filed with federal, state, or local government agencies, federal or state courts, and Better Business Bureaus.	Access Letter Q9e

DECLARATION OF DOUGLAS H. MEAL EXHIBIT D
COMPARISON OF ACCESS LETTER REQUESTS TO CID DOCUMENT REQUESTS

18	All minutes of Board of Directors meetings, executive committee meetings, or audit committee meetings of each Wyndham entity during the applicable time period.	
19	Documents sufficient to show the Company's policies and procedures relating to the retention and destruction of documents.	Produced in reponse to Access Letter Q5 b

EXHIBIT 3



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Lisa W. Schifferle
Attorney
Division of Privacy & Identity Protection

Direct Dial: 202.326.3377
Fax : 202.326.3768
E-mail: lschifferle@ftc.gov

April 8, 2010

BY EMAIL AND FEDERAL EXPRESS

Kirsten Hotchkiss
Senior Vice President - Legal and Assistant Secretary
Wyndham Hotels and Resorts, LLC
7 Sylvan Way
Parsippany, NJ 07054

Dear Ms. Hotchkiss:

As stated in my voice-mail message earlier today, the staff of the Federal Trade Commission ("Commission") is conducting a non-public investigation into Wyndham Hotels and Resorts, LLC's ("Wyndham") compliance with federal laws governing information security. According to recent news reports and statements issued by Wyndham,¹ sensitive personal information (including credit card information) of Wyndham's customers was obtained from Wyndham's computer networks by unauthorized individuals on three separate occasions since July 2008 (hereinafter "the three breaches"). We seek to determine whether Wyndham's information security practices comply with Section 5 of the Federal Trade Commission Act ("FTC Act"), which prohibits deceptive or unfair acts or practices, including misrepresentations about security and unfair security practices that cause substantial injury to consumers.²

¹ See, e.g. www.pcworld.com, *Wyndham Hotels Hacked Again* (Feb. 26, 2010), http://www.pcworld.com/businesscenter/article/wyndham_hotels_hacked_again.html; www.computerworld.com, *Losing Sleep over Three Data Breaches in a Year* (Mar. 5, 2010), http://www.computerworld.com/s/article/9166538/Losing_sleep_over_three_data_breaches_in_a_year.html; Wyndham Hotels and Resorts (Feb. 2010), http://www.wyndhamworldwide.com/customer_care/data-claim-faq.cfm.

² 15 U.S.C. § 45 *et seq.*

As part of our review, we ask that you provide us with the information and documents listed below on or before **May 10, 2010**. Please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. After we receive the information and documents, we will invite you to meet with Commission staff in our Washington, D.C. office or by telephone to further discuss this matter. In preparing your response:

- For purposes of this letter, "Wyndham" shall include Wyndham Hotels and Resorts, LLC, its parents, subsidiaries, divisions, affiliates, franchisees, hotels managed by franchisees that use the Wyndham trade name, and agents.
- Please provide all responsive documents within the possession, custody and control of Wyndham.
- Please submit *complete* copies of all documents and materials requested, even if you deem only a part of the document to be responsive.
- If any documents are undated, please indicate the date on which they were prepared or received by Wyndham.
- Please Bates stamp your response and itemize it according to the numbered paragraphs in this letter. If you have previously submitted documents, please refer to Bates number(s) in your itemized response to prevent unnecessary duplication.
- If you do not have documents that respond to a particular request, please submit a written statement in response. If a document provides only a partial response, please submit a written statement which, together with the document, provides a complete response.
- If you decide to withhold responsive material for any reason, including an applicable privilege or judicial order, please notify us before the date set for response to this request and submit a list of the items withheld and the reasons for withholding each.
- For purposes of this letter, the term "personal information" means individually identifiable information from or about an individual consumer, including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) a driver's license number; (g) financial account information, including account numbers or identifiers, and credit, debit, and/or ATM card information such as card number, expiration date, and data stored on a card's magnetic stripe; (h) a persistent identifier, such as a customer number held

in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information from or about an individual consumer that is combined with any of (a) through (h) above.

- Please note that we do not wish to receive files containing any individual consumer’s Social Security or driver’s license number, or financial account information. If you have responsive documents that include such information, please redact that information before providing us with the documents.
- We may seek additional information from you at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested below, but also any other information that concerns, reflects, relates to this matter, including files and information stored electronically, whether on computers, computer disks and tapes, or otherwise) until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.³ This request is not subject to the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.
- A responsible corporate officer or manager of Wyndham shall sign the responses and certify that the documents produced and responses given are complete and accurate.

REQUEST FOR DOCUMENTS AND INFORMATION

Please provide the documents and information requested below.⁴ Unless otherwise indicated, the time period covered by these requests is from **January 1, 2008** through the date of full and complete production of the documents and information requested.

³ Failure to retain documents that may be relevant to this matter may result in civil or criminal liability. 15 U.S.C. § 50.

⁴ For purposes of this letter the word “any” shall be construed to include the word “all,” and the word “all” shall be construed to include the word “any.” The word “or” shall be construed to include the word “and” and the word “and” shall be construed to include the word “or.” The word “each” shall be construed to include the word “every,” and the word “every” shall be construed to include the word “each.” The term “document” means any preexisting written or pictorial material of any kind, regardless of the medium in which such material was created, and regardless of the method by which it is stored (e.g., computer file, computer disk or tape, or microfiche).

General Information

1. Identify the complete legal name of Wyndham and all other names under which it does, or has done, business, its corporate mailing address, and the date and state of incorporation.
2. Identify and describe Wyndham’s parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchisees, operations under assumed names, and entities over which it exercises supervision or control. For each such entity, describe in detail the nature of its relationship to Wyndham and provide copies of any contracts regarding its relationship with Wyndham.
3. Provide documents sufficient to identify and describe in detail Wyndham’s business. The response should include but not be limited to: (a) the products and services Wyndham (including but not limited to hotels managed by franchisees that use the Wyndham trade name) offers, sells, or otherwise provides to customers; and (b) information identifying, annually, total revenue and total number of employees.
4. Identify the name, location, and operating system of each computer network Wyndham (including but not limited to its franchisees or other related entities) used to store, maintain, process, transmit, handle, or otherwise use (collectively hereinafter, “store and process”) personal information (such as to prepare, send, and receive authorization requests for credit and debit card transactions) as of January 1, 2008.
5. For each network identified in the response to Request 4, above:
 - (a) identify the type(s) of personal information stored and processed on the network, the source of each type of information (including, but not limited to: credit or debit cards; information provided by customers to obtain gifts or rewards; and information provided by third parties); and describe in detail how each type of information is stored and processed by Wyndham;
 - (b) provide:
 - (1) blueprints and diagrams setting out in detail the components, topology, and architecture of the network. Responsive documents should include, but not be limited to: documents that identify and locate the components of the network, such as computers; POS devices; cash registers; remote access equipment (such as wireless access points); servers; firewalls; routers; internet, private line, and other connections; connections to other Wyndham networks and outside networks; and

security mechanisms and devices (such as intrusion detection systems); and

(2) a narrative that describes in detail the components of the network and explains the functions of the components, and how the components operate together on the network;

- (c) provide documents setting out, and describe in detail, the security procedures, practices, policies, and defense(s) (such as access controls or encryption) in place to protect personal information from unauthorized access while stored on the network, transmitted within the network or between networks, and/or processed on the network;
- (d) provide all documents that concern, relate, or refer to security vulnerabilities in the network, including, but not limited to, documents identifying vulnerabilities, documents setting out and explaining the measures implemented to address the vulnerabilities, and communications, such as emails, that assess, question, or describe the state of security, warn of vulnerabilities, or propose or suggest changes in security measures; and
- (e) provide the name(s), title(s), and contact information of the individual(s) responsible for creating, designing, managing, securing, and updating the network.

The responses to each subpart of this Request should describe in detail each material change or update that has been made that concerns, refers, or relates to the subpart, as well as the date the change or update was implemented and the reason(s) for the change or update. If each network has the same standard framework, then you may provide one example rather than providing repeated copies of the same standard network.

- 6. Describe in detail, and provide documents setting out, the process(es) Wyndham (including but not limited to its franchisees or any other related entities outlined in response to Request #2) uses to provide authorization for credit or debit card transactions (“card authorization”). The response should:
 - (a) set forth the complete transmission or flow path for authorization requests and responses and the underlying information for each network involved in any way in card authorization, starting with the entity to whom a card is presented to pay for a purchase and including each intermediary on the path (including, but not limited to Visa, MasterCard, American Express, Discover [hereinafter collectively, “bank associations”]; acquiring, issuing, and other banks; Wyndham; third-party processors; merchant servicers; independent sales organizations; and

other entities) and final destination, and ending with receiving the response to the authorization request;

- (b) identify each portion of the transmission or flow paths set out in the response to Request 6(a), above, where authorization requests, authorization responses, or the underlying personal information are transmitted in clear text, if any, as well as the time period during which the requests, responses and information were transmitted in clear text;
- (c) identify the system(s), computer(s), or server(s) used to aggregate authorization requests in whole or in part and transmit them to bank associations and banks (“card authorization server”), and, for each server, identify the application(s) used for card authorization and the services enabled on the server, and describe in detail how the server has been protected from unauthorized access (such as protected by its own firewall);
- (d) describe in detail how and where authorization requests and responses and underlying personal information are stored or maintained (such as by being stored on a card authorization server or written to transaction logs located elsewhere on a network), as well as how stored or maintained requests, responses, and information have been protected from unauthorized access; and
- (e) identify and describe the number of authorization requests and responses that Wyndham received, forwarded, processed, stored, or transmitted for each month over the period in question, as well as the type of card presented to the merchant (such as credit or debit) and the disposition of the request (such as approved, declined, not completed, not authorized, or other classification, description, or category).

Information About the Three Breaches

In this section entitled “Information About the Three Breaches,” please respond to each of the questions breach by breach. In other words, answer Requests #7-12 for the first breach (July-August 2008), then answer Requests #7-12 for the second breach (March-May 2009), and then answer Request #7-12 for the third breach (October 2009-January 2010).

- 7. For each breach, describe in detail and produce documents sufficient to identify how and when Wyndham first learned about the breach.
- 8. Provide all documents prepared by or for Wyndham that identify, describe, investigate, evaluate, or assess: (a) how each breach occurred; (b) the time period over which it occurred; (c) where each breach began (*e.g.*, what the point of entry was and where it was located on the network); and (d) the path the

intruder followed from the point of entry to the information compromised and then in exporting or downloading the information (including all intermediate steps).

Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in each breach; reports of penetration and gap analysis; logs that record the intruder's steps in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was configured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of each breach prepared internally and by third-parties; and other records relating or referring to each breach, including minutes or notes of meetings attended by Wyndham's personnel and documents that identify the attacker(s).

9. Identify the name and location of each computer network on which personal information may have been accessed as a result of each breach, and for each such network describe in detail and provide all documents that relate to:
 - (a) the type(s) (*e.g.*, consumer's name, address, and payment card number, expiration date, and security code) and amount(s) of personal information that was or may have been obtained, including but not limited to the number of credit and/or debit card numbers;
 - (b) any subsequent unauthorized use of credit and/or debit cards alleged in any way to be linked to each instance of unauthorized access, including, but not limited to, the number of instances where credit and/or debit cards were used without the card holder's authorization, the dates of such use, and the amounts charged or debited.

Responsive documents should include, but not be limited to: fraud reports, alerts, or warnings issued by bank associations, banks, or other entities; lists identifying credit, debit, and other types of cards that have been used without authorization or may have been exposed by each breach as well as the issuing banks; documents that assess, identify, evaluate, estimate, or predict the amount of fraudulent purchases resulting from each breach; claims made against Wyndham's acquiring bank(s) under bank network alternative dispute resolution programs (*e.g.*, pre-compliance and compliance actions), and the resolution of any such claims; claims made against Wyndham by banks that issued cards that

have been used for unauthorized purchases (such as by demand letters); claims of fraud and/or identity theft, including, but not limited to, affidavits filed by consumers with their banks; and documents that assess, identify, evaluate, estimate, or predict the number of credit, debit, and other types of cards that have been cancelled and/or reissued, the cost per card and in total of cancelling and/or reissuing cards, and additional costs to Wyndham and/or third parties, attributable to each breach (such as for increased monitoring for fraud or providing fraud insurance to consumers affected by each breach);

- (c) the security procedures, practices, policies, and defenses in place when the first instance of each breach occurred as well as any changes to those security procedures, practices, policies, or defenses made thereafter;
- (d) each action Wyndham has taken in response to learning about the unauthorized access to personal information (*e.g.*, notifying consumers or law enforcement, improving security), including when the action was taken; and
- (e) investigations of or complaints filed with or against Wyndham that concern unauthorized access to personal information, including but not limited to correspondence with Wyndham and documents filed with: Federal, State, or local government agencies; Federal or State courts; and Better Business Bureaus.

10. According to news articles, at least one breach involved a hacker accessing a Wyndham data center through a franchisee.⁵

- (a) Identify which franchisees, subsidiaries, or data centers were involved in each of the three breaches.
- (b) For each such franchisee, subsidiary or data center identified in response to Request 10a, describe and provide documents relating to Wyndham's requirements regarding such entity's compliance with Wyndham's security practices.
- (c) For each such franchisee, subsidiary or data center identified in response to Request 10a, describe and provide documents relating to the network relationship between the entity and Wyndham, including but not limited to: who supplies such entity with its networks and/or who owns the

⁵ See, *e.g.* www.networkworld.com, *Hackers steal thousands of Wyndham credit card numbers* (Feb. 18, 2009), <http://www.networkworld.com/news/2009/021809-hackers-steal-thousands-of-wyndham-credit-card-numbers.html>.

networks; who maintains those networks; who sets security standards for those networks; who monitors those networks; who is responsible for security on those networks; and who is authorized to have access to those networks.

11. According to a statement by Wyndham,⁶ at least one breach may have affected consumers in countries outside of the United States.
 - (a) Describe in detail and provide documents sufficient to identify whether non-U.S. consumers' personal information was or may have been obtained and, if so, the types and amounts of information that was or may have been obtained; the country where the information was originally collected; and whether the information was originally collected by, came from, or was sent to an entity in a member country of the European Union.
 - (b) State whether Wyndham is a certified Safe Harbor company and, if so, identify the date of certification and provide all documents and information used by Wyndham as part of its application for certification under the program.
 - (c) Provide documents sufficient to identify, and describe in detail: all networks located outside of the United States used by Wyndham to store and process personal information; the physical location(s) of each network; and the function(s) and business purpose(s) of each network; and
 - (d) For each system identified in response to Request 11(c), above, describe in detail the extent and nature of any interconnection or interface with Wyndham networks located in the United States.
12. For each of the three breaches, identify how (such as by public announcement or individual breach notification letter), when, how many, and by whom customers were notified that their information was or may have been obtained without authorization. If notification has been made, explain why notification was made (*e.g.*, compelled by law) and provide a copy of each substantively different notification. If notification was not provided as soon as Wyndham became aware of each breach or was not provided to all affected customers or at all, explain why not.

⁶ See *supra* footnote 1. According to the FAQs on Wyndham's website, "the customers represent a cross-section of Wyndham's global customer base."

Other Information

13. Describe and provide copies of each different policy adopted and statement made by Wyndham to consumers regarding the collection, disclosure, use, and protection of their personal information or customer information, including any policies and statements relating to the privacy or security of such information, and for each policy or statement, identify the date(s) when it was adopted or made, and describe all means by which it was distributed.
14. Describe in detail and provide documents sufficient to identify any other instances (besides the three breaches) of unauthorized access to Wyndham's computer system of which you are aware, as well as the types of information accessed without authorization and when the unauthorized access occurred.

In addition to these categories of documents and information, please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. Any materials you submit in response to this request, and any additional information provided it is marked "Confidential," will be given confidential treatment.⁷ We may also seek additional information at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested above, but also any other information relating to this matter, including files and information stored on computers or on computer disks and tapes) until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.⁸ This request is not subject to the requirements of the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.

Please send all documents and information to: Lisa W. Schifferle, Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Avenue, NW, Mail Stop NJ-3137, Washington, D.C. 20580. Due to extensive delays resulting from security measures taken to ensure the safety of items sent via the U.S. Postal Service, we would very much appreciate receiving these materials via Federal Express or a similar delivery service provider, if possible.

⁷ The Commission's procedures concerning public disclosure and confidential treatment can be found at 15 U.S.C. Sections 46(f) and 57b-2, and Commission Rules 4.10-4.11 (16 C.F.R. Sections 4.10-4.11 (1984)).

⁸ Failure to retain any documents that may be relevant to this matter may result in civil or criminal liability.

Thank you for your prompt attention to this matter. Please call me at 202-326-3377 or Molly Crawford at 202-326-3076 if you have any questions about this request or need any additional information.

Sincerely,

/s/ Lisa W. Schifferle

Lisa W. Schifferle
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission

EXHIBIT 4

DECLARATION OF KORIN NEFF, ESQ.

1. My name is Korin Neff. I make this Declaration in support of the Petition to Quash filed before the Federal Trade Commission (“FTC”) by Wyndham Worldwide Corporation (“WWC”) and Wyndham Hotels & Resorts LLC (“WHR” and, jointly with WWC, “Wyndham”).

2. I am over 18 years old and competent to make this Declaration.

3. I am currently the Group Vice President for Global Privacy at WWC. I have held this position since June 2010. Before that, I worked as Vice President-Legal at WWC.

4. I have reviewed the CID the FTC issued to WWC in the FTC’s investigation of WHR’s information security practices (the “WHR Investigation”). Based on my understanding of the requests contained in the CID, I believe that it will be very costly and time-consuming for Wyndham to respond to the CID.

5. While Wyndham cannot precisely quantify the costs that would be incurred in responding to the CID before documents are searched for and reviewed, Wyndham believes it can reasonably estimate those costs and has made an effort to do so. In developing that estimate, Wyndham used the costs of WHR’s voluntary cooperation with the WHR Investigation as a starting point.

6. In April 2010, the FTC sent a voluntary access letter to WHR in connection with this investigation. The letter sought responses to written questions and the production of documents from WHR.

7. The process followed by WHR for providing written and oral responses to the questions posed in the access letter and in subsequent communications from the FTC involved extensive fact development interviews conducted by in-house and outside counsel, drafting of responses, and re-checking the responses for accuracy. The process by which WHR collected, searched for, reviewed, and produced documents requested in the access letter and in subsequent communications from the FTC included identifying key custodians who might have relevant and responsive information, collecting and preserving documents with electronically stored data (“ESI”) and hard copy documents, testing potential search terms for accuracy, engaging a vendor to perform searches to identify documents potentially responsive to the FTC’s voluntary access requests, reviewing those documents for responsiveness and privilege, engaging a vendor to process and Bates stamp the documents, and providing the aforementioned documents to the FTC. All of these steps involved extensive involvement of outside counsel in addition to in-house counsel, other employees, and an electronic discovery vendor.

8. I have requested and received information about the out-of-pocket costs incurred in responding to the requests made by the FTC in the voluntary access letter and subsequent communications. Those costs are estimated to be not less than \$5 million.

- a. ESI Review: \$2.8 million
- b. Non-ESI Response to Access Letter: \$2.2 million

This figure does not include other costs, such as the time lost by various employees in addressing the FTC’s requests.

9. The costs involved in ESI review include:

- a. Collection of documents
- b. Processing of documents by an outside vendor
- c. Development of search terms and review methodology
- d. Review of documents for responsiveness and privilege
- e. Processing of documents by an outside vendor for a production
- f. Hosting of data by vendor in on document review platform

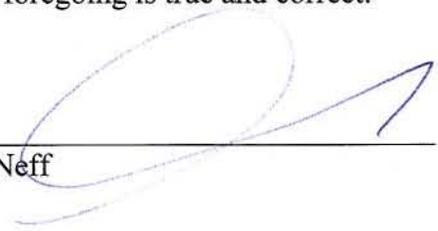
10. Though the CID is significantly duplicative of the requests made by the FTC in the access letter and subsequent communications, Wyndham estimates that compliance with the “all-document requests” contained in the CID would require a full review of the electronic files of three additional custodians.

11. Wyndham estimates that a full review of the electronic files of three additional custodians would cost approximately \$1 million and take approximately 10 weeks to complete. If Wyndham were required to review the electronic files of more than three additional custodians in order to respond to the CID’s all-document requests (as the FTC has argued should be the case), Wyndham estimates the cost of the ESI review would increase by approximately \$350,000, and the duration of the ESI review would increase by approximately 2.5 weeks, for each additional custodian.

12. Wyndham estimates that the cost to prepare a meaningful response to the rest of the CID’s discovery requests (i.e., the CID’s interrogatories and “sufficient to describe” document requests), and to prepare the privilege log called for by the CID, would be not less

than \$2.75 million, and at least 6 months of work would to be needed to prepare both such a response (which would not be complete) and the requested privilege log.

I declare under penalty of perjury of that the foregoing is true and correct.



Korin Neff

Executed on January 20, 2011

EXHIBIT 5

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of)
)
)
WYNDHAM WORLDWIDE CORPORATION,)
a corporation,)
)
WYNDHAM HOTEL GROUP, LLC,)
a limited liability company,)
)
WYNDHAM HOTELS & RESORTS, LLC,)
a limited liability company,)
)
and)
)
WYNDHAM HOTEL MANAGEMENT, INC,)
a corporation.)
_____)

DOCKET NO. C-

COMPLAINT

The Federal Trade Commission, having reason to believe that Wyndham Worldwide Corporation, Wyndham Hotel Group, Wyndham Hotels and Resorts, and Wyndham Hotel Management (hereinafter, “respondents”) have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

- 1. Respondent Wyndham Worldwide Corporation (“Wyndham Worldwide”) is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsipanny, NJ 07054. At all relevant times, Wyndham Worldwide has been in the hospitality business, franchising and managing hotels.
- 2. Respondent Wyndham Hotel Group (“The Hotel Group”) is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsipanny, NJ

07054. The Hotel Group is a wholly-owned subsidiary of Wyndham Worldwide, and through its subsidiaries it franchises and manages approximately 7,000 hotels under twelve hotel brands, one of which is the Wyndham brand.

3. Respondent Wyndham Hotels and Resorts (“Wyndham Hotels”) is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany, NJ 07054. Wyndham Hotels is a wholly-owned subsidiary of The Hotel Group, and it licenses the Wyndham name to approximately seventy-five independently-owned hotels under franchise agreements.
4. Respondent Wyndham Hotel Management (“Hotel Management”) is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, NJ 07054. Hotel Management is also a wholly-owned subsidiary of The Hotel Group, and it licenses the Wyndham name to approximately fifteen independently-owned hotels under management agreements.
5. The acts and practices of respondents as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.
6. In conducting their business, including taking reservations and accepting payment for guest stays, respondents and the hotels licensed to use the Wyndham name by Wyndham Hotels and Hotel Management (collectively, hereinafter “Wyndham-branded hotels”) routinely collect and store personal information from consumers, including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes (hereinafter “personal information”).
7. Under their franchise and management agreements, Wyndham Hotels and Hotel Management require each Wyndham-branded hotel to purchase a designated property management system – a computer network that handles reservations, checks guests in and out, assigns rooms, manages room inventory, and handles accounting and billing. Each Wyndham-branded hotel’s property management system is managed by Wyndham Hotels, and is linked to Wyndham Hotels’ own central reservation system, which coordinates reservations across the Wyndham brand.
8. Wyndham Hotels’ information security program and the management of the Wyndham-branded hotels’ property management systems were handled by The Hotel Group until June 2009, and thereafter by Wyndham Worldwide.
9. Since at least 2008, respondents have disseminated or caused to be disseminated privacy policies or statements on their website, including but not limited to, the following statement regarding the privacy and confidentiality of customer information:

We safeguard our Customers’ personally identifiable information by using industry standard practices. . . . We take commercially

reasonable efforts to create and maintain “fire walls” and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed. (See Exhibit A).

10. Since at least April 2008, respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information collected and maintained by Wyndham Hotels and the Wyndham-branded hotels. Among other things, respondents:
 - (a) failed to use readily available security measures to limit access between Wyndham-branded hotels’ computer networks and the Wyndham Hotels’ centralized computer network, such as by employing firewalls;
 - (b) failed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures, thus permitting them to create an unnecessary risk by storing personal information, including payment card information, in clear, readable text;
 - (c) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks or to conduct security investigations, such as by monitoring system logs or adequately investigating multiple account lockouts;
 - (d) failed to follow proper incident response procedures, including failing to monitor Wyndham Hotels’ computer network for malware used in a previous intrusion; and
 - (e) failed to adequately restrict third-party vendors’ access to Wyndham Hotels’ network and the networks of the Wyndham-branded hotels, such as by restricting connections to specified IP addresses or granting temporary, limited access.

11. As a result of these failures, between April 2008 and January 2010, intruders gained access to Wyndham Hotels’ and the Wyndham-branded hotels’ computer networks on three separate occasions. The intruders were able to access sensitive personal information stored on their networks, including payment card account numbers, expiration dates, and security code numbers.
 - (a) Respondents first became aware that intruders had gained unauthorized access to Wyndham Hotels’ network and the networks of forty-one of the Wyndham-branded hotels in September 2008. The intruders installed memory-scraping malware on these networks, thereby accessing payment card data that was present temporarily on their servers. In addition, the intruders located files on some of the Wyndham-branded hotels’ networks that contained payment card account information for large numbers of consumers in clear text. Respondents’

investigation determined that information for more than 500,000 payment card accounts was likely accessed during this incident.

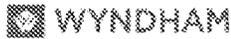
- (b) In May 2009, respondents learned that intruders had again installed memory-scraping malware on Wyndham Hotels' network and on the networks of twenty Wyndham-branded hotels. In addition, the intruders re-configured some of the Wyndham-branded hotels' software so that new payment card information would be stored in clear text and accessible during the intrusion. In this incident, the intruders were able to access information for more than 50,000 payment card accounts.
 - (c) In January 2010, respondents again learned that intruders had installed memory-scraping malware on Wyndham Hotels' network and the networks of twenty-eight Wyndham-branded hotels. As a result, the intruders were able to access information for approximately 69,000 payment card accounts.
12. These data security incidents compromised more than 619,000 payment card accounts used by consumers and resulted in fraudulent charges on some of these implicated accounts.
 13. Through the means described in Paragraph 9, respondents represented, expressly or by implication, that respondents had implemented reasonable and appropriate measures to protect personal information against unauthorized access.
 14. In truth and in fact, as represented in Paragraph 10, respondents did not implement reasonable and appropriate measures to protect personal information against unauthorized access. Therefore, the representations set forth in Paragraph 13 were, and are, false or misleading, and constitute a deceptive act or practice.
 15. The acts and practices of respondents as alleged in this complaint constitute deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this ___ day of ____, 2011, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

EXHIBIT A



Privacy Policy

PRIVACY POLICY

Introduction

**WYNDHAM HOTEL GROUP, LLC
CUSTOMER PRIVACY POLICY
AND INFORMATION PRACTICES STATEMENT
Revised May 2008**

Wyndham Hotel Group, LLC, ("WHG"), a subsidiary of Wyndham Worldwide Corporation ("WWC"), is the parent company of Wyndham Hotels and Resorts, LLC., Days Inns Worldwide, Inc., Howard Johnson International, Inc., Ramada Worldwide Inc., Super 8 Worldwide, Inc., Travelodge Hotels, Inc., Wingate Inns International, Inc., AmeriHost Franchise Systems, Inc., Knights Franchise Systems, Inc., and Baymont Franchise Systems, Inc. (collectively, the "Franchisors") which license the Wyndham®, Days Inn®, Howard Johnson®, Ramada®, Super 8®, Travelodge®, Wingate® by Wyndham, AmeriHost Inn®, Knights Inn®, and Baymont Inn & Suites® hotel systems (collectively, the "Brands") to independently owned hotels ("Franchisees"). Travel Rewards, Inc., the sponsor of the Wyndham RewardsSM guest loyalty program, is also a wholly owned subsidiary of WHG. Wyndham Hotels and Resorts, LLC, one of the Franchisors, is the sponsor of the Wyndham ByRequest® guest loyalty program. In this Privacy Policy WHG, the Franchisors, Wyndham Vacation Resorts, each of their affiliates, the Brands, Wyndham Rewards and Wyndham ByRequest, may be referred to collectively, as "Wyndham", "we", "us" or "our." Wyndham Rewards, Wyndham ByRequest, and any successor or additional guest loyalty programs may collectively be referred to as "Loyalty Programs."

We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Programs (collectively "Customers"). Examples of individual-specific information ("Information") are described in the Section, "What is Individual Specific Information?" We have adopted this Customer Privacy Policy to guide how we utilize Information about our Customers. This Policy will evolve and change as we continue to study privacy issues.

Application

This policy applies to residents of the United States, hotels of our Brands located in the United States, and Loyalty Program activities in the United States only. We do not accept the jurisdiction of any other laws over the above. This policy also applies only to our Customers. We have a separate policy governing any internet sites or extranet sites accessible only to the Franchisees and/ or Brands

Purpose

Our purpose in establishing this policy is to balance our legitimate business interests in collecting and using Information with our Customers' reasonable expectations of privacy. Our intent is to bring you offers and discounts that we believe are relevant to your interests. We believe that our Customers benefit from promotional activity based on Customer Information employed to market goods and services offered by and through us and our other affiliates and business units. For more information on our affiliates, check the WWC corporate Web site, www.wyndhamworldwide.com

Security

We collect Information only in a manner deemed reasonably necessary to serve our legitimate business purposes and comply with our legal obligations. We safeguard our Customers' personally identifiable information by using industry standard practices. Although "guaranteed security" does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such Information consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information - such as credit card numbers, online forms, and financial data - from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed. Our privacy protection practices help us to maintain accurate, timely, complete and relevant information for our business purposes. Our communication system, software and database practices have been designed to aid us in supporting authenticity, integrity and confidentiality. Although we use commercially reasonable efforts to maintain data security when data is transmitted through third party communication service providers, we do not warrant the security of data during such transmission. Third party Web sites that are accessed through links, banners and other means of electronic connection on our Web

sites have separate privacy and data collection practices, and security measures. We have no control over these third party Web sites and no responsibility or liability for the practices, policies and security measures implemented by third parties on their Web sites. These third party Web sites have content, advertising, banners, links, sponsors, partners and connections over which we have no control and no responsibility. We encourage you to contact these third parties to ask questions about their terms of use, privacy practices, policies and security measures before disclosing personal information on linked Web sites. We do not endorse or approve the content, terms of use, privacy policy, advertising or sponsors of any linked Web site. Please click on this link [Feedback/Opt out](#) to give us your feedback about this Policy or opt out of further communications from us.

The Internet

On our Web sites we do not collect personally identifiable information from Customers unless they provide it to us voluntarily and knowingly. When you reserve a room with us we will capture information such as name, address, telephone number, e-mail address, and credit card number to process your reservation. The primary purpose of capturing your e-mail address when you make a reservation with us is to send you a reservation confirmation. The confirmation may contain additional offers that we believe may be of interest to you, based on the information you provide to us. If you have consented to be put on our e-mail lists, we may contact you via e-mail from time to time. You will always be provided with a way to opt-out of future e-mailings. However we will continue to send e-mails to confirm your reservations.. Like many other Internet sites, we automatically collect certain non-personal information regarding our Customers, such as software client information (for example, IP addresses, browser versions and operating systems) and aggregate information (for example, number of pages accessed) in order to analyze Web traffic and usage trends, and to enable us to tailor content and services to provide a better fit to our Customers' needs. Information of this nature does not pertain to your specific identity and is not associated with your personal information. Our Web sites have hyperlinks that connect the Customer to other Web sites, some of which are not affiliated with or controlled by us. Once you leave our Web sites, each new Web site you visit may have its own privacy policy and terms of use. Your interaction with these sites will not be governed by this policy or the terms of use of our Web sites. Access to and use of such linked Web sites through links provided on this Web site is governed by the privacy policies and terms of use and policies of those Web sites.

Cookies

We may place a "cookie" on your web browser. A cookie is a very small text file that is sent to a Customer's browser from a web server and stored on the Customer's computer hard drive. It assigns the computer a unique identifier. The cookie stores information on your hard drive so we can communicate with you more efficiently, respond to you based on prior sessions at which you provided information about you or your preferences to us and understand what you prefer to view on our Web sites. We do not use cookies to store passwords or credit card information. Cookies do not tell us your individual identity unless you have chosen to provide it to us. Your browser may be set to allow you to be notified when a cookie is to be placed on your browser, decline the cookie or delete cookies that have been placed on your browser. Some functions of our Web sites may not work or may work slowly if a cookie is refused. Our Web site uses third party service providers to serve and host our advertisements. These third parties may place cookies on your computer if you click on or access the advertising. The third party cookies are used to track whether the site was accessed from the advertisement. The cookies generated from the advertisements do not contain personally identifiable information. We do not control these cookies and they may not follow the rules we have set for our own cookies. We and our third party ad server also use invisible pixels, sometimes called web beacons, on our Web site to count how many people visit certain web pages. Information collected from invisible pixels is used and reported in the aggregate without the use of a Customer's personally identifiable information. This information may be used to improve marketing programs and content and to target our Internet advertisements on our site and other Web sites. For more information about our third party ad server, or to learn your choices about not having this non-personal information used to serve ads to you, [please read a brief overview of our third party ad server's Privacy Policy](#).

The Information We Collect

If you make a reservation through our central reservation center or a Brand Web site or if you join one of our Loyalty Programs, we will collect and store your name, address and other basic information about you for the purpose of reserving the hotel accommodations or making the Loyalty Program benefits available to you. If you make a hotel reservation directly with a Brand Franchisee, state law in many states requires the hotel operator to collect and retain your name, address, telephone number and other basic information solicited on the hotel registration card and make it available to law enforcement officers. Our hotel operators send this information, as well as e-mail address and transaction detail (what goods and services were charged on the hotel bill) to our enterprise data warehouse or other data storage facility for collection and storage (the 'Data Warehouse'). In addition, we obtain personally identifiable information from third party sources that are obligated to comply with applicable privacy laws and append it to the information maintained in the Data Warehouse about you. Credit card numbers used for payment or guarantee are automatically encrypted in our Data Warehouse so that they cannot be easily accessed. We do not collect Social Security or driver's license numbers from Customers.

Feedback/Opt out

We offer Customers the opportunity to "opt-out" of communications. A customer may elect to opt out of receiving communications by following the directions posted on the e-mail communication or by visiting the Brand or the Loyalty Program Web site, by contacting the Customer Care Department of the Brand that was

patronized, or by contacting the Wyndham Rewards® Member Services Department. However, we will continue to send e-mails to confirm your reservations. Customers can elect to opt out from any of the following: (1) Mail - e-mail (excluding confirmation e-mails) and direct mail; (2) Phone -telephone and fax solicitation; or (3) Contact - all communications including e-mail, direct mail, fax and telephone. We maintain telephone "do not call" lists as mandated by law. We incorporate into our Data Warehouse "do not call" and "do not mail" lists maintained by other organizations. We process requests to be placed on do not mail, do not phone and do not contact lists within 60 days after receipt, or such shorter time as may be required by law. Any Customer may opt out of receiving communications by contacting us using the following methods:

By e-mail, [click here](#) to opt out.

By phone -

- x 888-564-4487 for AmeriHost Inn;
- x 877-212-2733 for Days Inn;
- x 877-222-3297 for Howard Johnson;
- x 877-225-5637 for Knights Inn;
- x 877-227-3557 for Ramada Inn;
- x 877-244-7633 for Super 8;
- x 877-321-7653 for Travelodge;
- x 877-333-6683 for Wingate by Wyndham;
- x 800-870-3936 for Baymont Inn;
- x 866-850-3070 for Wyndham Hotels and Resorts;
- x 866-996-7937 for Wyndham Rewards or Wyndham ByRequest.;
- x 888-877-0675 for Microtel Inn & Suites;
- x 888-297-2778 for Hawthorn Suites;

By mail - Opt Out/ Privacy, Hotel Group Wyndham Hotel Group, LLC 1 Sylvan Way Parsippany, NJ 07054

We also invite your feedback and comments on this Policy. Please contact us at the e-mail address or telephone number above or by writing to us at:

Privacy Policy Inquiry.
Wyndham Hotel Group,
1 Sylvan Way,
Parsippany, NJ 07054.

Reservations

When a Customer calls our reservation centers or contacts us via the Internet, fax or other means about hotel reservations, we need certain information such as name, address and telephone number to respond to the inquiry and to make the reservation. This information is sent to the hotel where the reservation is also recorded. A credit card number is necessary to guarantee the reservation past a certain time. The franchisee will charge the credit card account of a Customer who fails to arrive and fails to cancel the reservation in a timely manner. Franchisees may impose other conditions on the reservation such as minimum length of stay, advance deposit and other terms of the contract. A Customer should always ask for and record a confirmation number when making, changing or canceling a reservation. Information collected as part of the reservation process is used as this Policy describes whether or not the Customer actually utilizes the hotel reservation. The Franchisor may, but is under no obligation to, contact Customers with reservations to inform them about changes in the status of the hotel for which the reservations are made and may suggest alternative accommodations.

e-mail

We will ask Customers to submit their e-mail address when they make a hotel reservation with us or enroll in a Loyalty Program. The primary purpose for capturing your e-mail addresses when you make a reservation with us is to send you a reservation confirmation. Our confirmations may contain additional offers based on information you provide and your destination. The primary purpose for capturing your e-mail address when you enroll in a Loyalty Program is to send you on-line account statements. Whether Customers provide their e-mail address to us in order to make a hotel reservation or to enroll in a Loyalty Program, they may consent to receive e-mail offers from or through us, the Brands and our other affiliates. We may also collect Customer e-mail addresses and share them with our third party service providers for purposes of conducting consumer research and surveys as more fully described below. Customers will always have the ability to opt-out of future e-mail communications; however, we will continue to send e-mails to confirm your reservations. It is our intent to only send e-mail communications (other than confirmation e-mails and e-surveys) to Customers who have consented to receive them and/or to Customers who have permitted third parties to share the Customer's e-mail address for purposes of receiving promotional e-mails. At any time a Customer may opt-out of receiving e-mail communications by notifying us as provided in the Feedback/Opt-Out section above. We currently use third party e-mail service providers to send e-mails. This service provider is prohibited from using our Customer's e-mail address for any purpose other than to send Brand related e-mail.

SWEEPSTAKES / CONTESTS:

Occasionally we run sweepstakes and contests. We ask Customers who enter in the sweepstakes or contest to provide contact information (like an e-mail address). If a Customer participates in a sweepstakes or contest, his/her contact information may be used to reach him/her about the sweepstakes or contest, and for other promotional, marketing and business purposes. All sweepstakes/contests entry forms will provide a way for participants to opt-out of any communication from the sweepstake's/contest's administrator that is not related

to awarding prizes for the sweepstake/contest.

DIRECT MAIL / OUTBOUND TELEMARKETING:

Customers who supply us with Information, or whose Information we obtain from third parties, may receive periodic mailings or phone calls from us with information on our products and services or upcoming special offers/events. We offer our Customers the option to decline these communications. Customers may contact us to opt-out of such communications by notifying us as provided in the Feedback/Opt-Out section above.

RESEARCH/SURVEY SOLICITATIONS

From time to time we may perform research (online and offline) via surveys. We may engage third party service providers to conduct such surveys on our behalf. All survey responses are voluntary, and the information collected will only be used for research and reporting purposes to help us to better serve Customers by learning more about their needs and the quality of guest experience at our hotels and/or their experience with the Loyalty Programs. We may contact a Customer to inquire or survey him/her about his experience with a Loyalty Program or a Brand hotel visited and the prospect of future stays or the improvements needed to attract additional business from the Customer. The survey responses may also be used to determine the effectiveness of our Web sites, various types of communications, advertising campaigns, and/or promotional activities. If a Customer participates in a survey, the information given by the Customer will be used along with that of other study participants (for example, a Franchisor might report that 50% of a survey's respondents are males). We may share anonymous individual and aggregate data for research and analysis purposes. Participation in surveys is voluntary. Participants who do not wish to receive e-mail communications may opt-out of the receipt of such communications by notifying us as provided in the Feedback/Opt-Out section above.

What is Individual Specific Information?

Individual-specific or personally identifiable information is any information or data about a Customer that in itself, or as part of a unique combination of information, specifically recognizes the Customer by a unique identifier or descriptor. Examples of individual-specific include name, address, telephone number, e-mail address, employment status, credit card type and number, and other financial information.

What We Won't Do With Customer Information.

We will not:

1. Sell or rent Information to parties outside the Wyndham family of present or former companies (not including businesses that entered into long term contracts with us to obtain Customer Information, such as the Affinion Loyalty Group, or that entered into such contracts while a part of the Wyndham family and which later leave the family), our franchisees and affiliates, or allow our affiliates to sell or rent the Information to parties outside the Wyndham family of present and former companies, franchisees and affiliates;
2. Use the Customer Information we collect and store to make decisions about granting or extending consumer credit unless the Customer submits a separate credit application and authorizes us to use or disclose this information;
3. Act as a consumer reporting agency, or furnish information about any Customer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to any consumer reporting agency;
4. Maintain in our Data Warehouse any Information about any Customer on billing, collection or payment disputes with any franchisee, creditor or affiliate;

What We Will Do With Customer Information:

We will:

1. Use Customer Information to solicit additional hotel stays at the same hotel and other locations of the Brand, participation in the Loyalty Program, and to offer goods and services we believe may be of interest to Customers on behalf of ourselves, other non-hotel business units, our affiliates and former affiliates. For Customers who are Loyalty Program members, these solicitations may include offers from third party merchants that provide point earning or reward redemption opportunities in connection with the Program ("Loyalty Program Participants"). With Loyalty Program members' consent, we may provide their Customer information to the Loyalty Program Participants for purposes of them directly offering their goods and services to the members.
2. Include information about Customers gathered from other sources we believe to be reliable to identify our Customers more thoroughly and update Information we store and provide to third parties when the information changes, such as changes of address or new credit card expiration dates
3. Provide the name, address, telephone number and transaction Information, including payment method, about Customers to our and the Loyalty Programs' designated affinity credit card issuer(s) for use in the preselection process for the credit cards;
4. Create and use aggregate Customer data that is not personally identifiable to understand more about the common traits and interests of our Customers;
5. Use Customer Information to enforce a contract with us or a Franchisee or any Terms of Use of our Web sites, or provide access or disclosures that we believe in good faith are required to comply with

- applicable law (See Compliance with Law in this Policy);
6. Provide information on corporate credit card usage to the corporate card issuer or holder Customer directly or through third parties;
 7. Transfer Customer Information to the party that acquires the business or assets to which the information relates.
 8. Transfer and disclose Customer Information to our affiliates and subcontractors who administer the Loyalty Programs on our behalf or as we deem necessary to maintain, service, and improve services.

Our Franchisees.

Each Brand hotel is owned and operated by an independent Franchisee that is neither owned nor controlled by us or our affiliates. Each Franchisee collects Customer Information and uses the Information for its own purposes. We do not control the use of this Information or access to the Information by the Franchisee and its associates. The Franchisee is the merchant who collects and processes credit card information and receives payment for the hotel services. The Franchisee is subject to the merchant rules of the credit card processors it selects, which establish its card security rules and procedures. This policy does not apply to a Franchisee's Web site. Franchisees may also use e-mail campaigns and other methods of telephone, electronic, and direct mail solicitation without our consent or knowledge and are solely responsible for their content and methods of identifying and contacting addressees.

Other Disclosures/Compliance with Law.

We may be obligated to disclose Information about you to a law enforcement agency or by a court order, or under the discovery process in litigation, investigations, and prosecutions. We may provide Information to assist a Franchisee to enforce a contact you may have breached. We may also disclose information voluntarily to cooperate with law enforcement agencies in matters of national security. We may ask certain questions to comply with certain laws if you reside outside the United States or meet certain other criteria established by law or executive order. Unless otherwise prohibited by law or our contractual obligations, we may disclose personal information if required to do so by law, court order, or as requested by a governmental or law enforcement authority, or in good faith belief that disclosure is otherwise necessary or advisable. Situations may include: to perform, maintain or enforce contracts with our Customers, to protect the rights or properties of our Franchisees, affiliates and business partners, our Customers or others, or when we have reason to believe that disclosing the information is necessary to identify, contact or bring legal action against someone who may be causing or who may be threatening to cause interference with or damage to our rights properties, or the hotels in our Brands, whether intentionally or otherwise, or when anyone else could be harmed by such activities.

Correction

We make repeated efforts to verify the accuracy of Information and to correct and update our database from Information available to us. In the event a Customer believes that such Information held by us is inaccurate or outdated, we will, upon notification and sufficient time for verification, take all reasonable steps to correct any inaccuracy or update outdated information of which we are made aware.

Downloading

Please feel free to download or copy this Policy. You may obtain a copy free of charge by writing to us at Customer Privacy Policy, Wyndham Hotel Group, 1 Sylvan Way, Parsippany, NJ 07054.

Policy Changes.

The Policy in effect at the time of each visit to a Brand Web site applies to that visit. However, we may change or terminate this Policy at any time without prior notice by posting an amended version of the Policy on our Web site and providing you with the ability to opt out of any new, unanticipated uses of Information not previously disclosed in the Policy. Please check our Policy each time you visit our Web site or more frequently if you are concerned about how your Information will be used.

[Site Map](#) ; [About Wyndham Hotels and Resorts, LLC](#) ; [Wyndham Worldwide Corporation](#)
[Franchise Opportunities](#) ; [Wyndham Vacation Ownership](#) ; [Employment Opportunities](#)
[Wyndham at Home](#) ; [Travel Agent Services](#) ; [Women On Their Way](#) ; [Wyndham Green](#)
[Join Affiliate Program](#) ; [Privacy Policy](#) ; [Terms of Use](#)
©2010 Wyndham Hotels and Resorts, LLC

E-mail me exclusive Wyndham offers. | [Sign Up Now](#)

EXHIBIT 6

New Jersey 07054. Wyndham Hotel Group, LLC is a wholly-owned subsidiary of Wyndham Worldwide Corporation.

3. Proposed respondent Wyndham Hotels and Resorts, LLC is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. Wyndham Hotels and Resorts, LLC is a wholly-owned subsidiary of Wyndham Hotel Group.
4. Proposed respondent Wyndham Hotel Management, Inc. is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. Wyndham Hotel Management, Inc. is a wholly-owned subsidiary of Wyndham Hotel Group, LLC.
5. Proposed respondents admit all the jurisdictional facts set forth in the draft complaint.
6. Proposed respondents waive:
 - A. any further procedural steps;
 - B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and
 - C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.
7. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondents, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.
8. This agreement is for settlement purposes only and does not constitute an admission by proposed respondents that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.
9. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondents, (1) issue its complaint corresponding in form and substance

with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondents' addresses as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondents waive any right they may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.

10. Proposed respondents have read the draft complaint and consent order. Proposed respondents understand that they may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. "Personally identifiable information" or "personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (1) a first and last name; (2) a home or other physical address, including street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other state-issued identification number; (7) a financial institution account number; (8) credit or debit card information, including card number, expiration date, and security code; (9) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (10) any information that is combined with any of (1) through (9) above.
2. "Wyndham Hotels" shall mean Wyndham Hotels & Resorts, LLC, its subsidiaries, divisions, successors, and assigns.
3. "Hotel Management" shall mean Wyndham Hotel Management, Inc., its subsidiaries, divisions, successors, and assigns.
4. "The Hotel Group" shall mean Wyndham Hotel Group, LLC, and its successors and assigns.

5. Unless otherwise specified, “respondents” shall mean (1) Wyndham Hotels; (2) Hotel Management; (3) The Hotel Group; and (4) Wyndham Worldwide Corporation and its successors and assigns.
6. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
7. “Wyndham-branded hotel” shall mean an independently-owned hotel licensed to use the Wyndham name that is operated in the United States under a management or franchise agreement with Wyndham Hotels or Hotel Management.
8. “Franchisor Standard” shall mean any written standard, specification, policy, or procedure contractually applicable to Wyndham-branded hotels, and enforceable exclusively by respondents through their franchise and management agreements with the persons or entities who control Wyndham-branded hotels. A Franchisor Standard shall include, but not be limited to, “system standards” as defined under respondents’ franchise or management agreements with the persons or entities who control Wyndham-branded hotels.
9. “Hotel Network” shall mean any portion of a Wyndham-branded hotel’s computer network(s) that has routable connectivity to respondents’ computer network(s), either directly or indirectly, such as through a cloud service provider.
10. “Quality Assurance Program” refers to the program that evaluates the Wyndham-branded hotels’ compliance with certain Franchisor Standards by means of periodic inspections of the Wyndham-branded hotels.

I.

IT IS ORDERED that respondents, their officers, employees, agents, representatives, and all other persons or entities in active concert or participation with them who receive actual notice of this order by personal service or otherwise, directly or through any corporation, subsidiary, division, website, or other device, shall not misrepresent in any manner, expressly or by implication, the extent to which any respondent maintains or protects the privacy, confidentiality, security, or integrity of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that The Hotel Group, Wyndham Hotels, and Hotel Management shall, no later than the date of service of this order, establish and implement, and

thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to The Hotel Group's, Wyndham Hotels' and Hotel Management's size and complexity, the nature and scope of their activities, and the sensitivity of the personal information that they collect from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from The Hotel Group, Wyndham Hotels, and Hotel Management and requiring such service providers by contract to implement and maintain appropriate safeguards for such information; and
- E. the evaluation and adjustment of their information security programs in light of the results of the testing and monitoring required by subpart C, any material changes to their operations or business arrangements, or any other circumstances that they know or have reason to know may have a material impact on the effectiveness of their information security program.

III.

IT IS FURTHER ORDERED that Wyndham Hotels shall adopt a Franchisor Standard contractually obligating each person or entity who controls a Wyndham-branded hotel to

establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information maintained on or transmitted to or through the Hotel Network of the Wyndham-branded hotel.

- A. Wyndham Hotels shall adopt such a Franchisor Standard within ninety (90) days after the date of service of this order.
- B. Such Franchisor Standard shall require that each Wyndham-branded hotel establish and implement its comprehensive information security program no later than ninety (90) days after such Franchisor Standard becomes applicable to it.
- C. Such Franchisor Standard shall require the content and implementation of each Wyndham-branded hotel's comprehensive information security program to be fully documented in writing, and shall require each such program to contain administrative, technical, and physical safeguards appropriate to the size and complexity of that Wyndham-branded hotel, the nature and scope of its activities, and the sensitivity of the personal information that it collects from or about consumers, to the extent such information is maintained on or transmitted to or through its Hotel Network. Such Franchisor Standard shall require:
 - 1. the designation of an employee or employees to coordinate and be accountable for the Wyndham-branded hotel's information security program;
 - 2. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;
 - 3. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

4. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive and requiring such service providers by contract to implement and maintain appropriate safeguards for such information; and
 5. the evaluation and adjustment of each Wyndham-branded hotel's information security program in light of the results of the testing and monitoring required by subpart 3, any material changes to its operations or business arrangements, or any other circumstances that the Wyndham-branded hotel knows or has reason to know may have a material impact on the effectiveness of its information security program.
- D. Through its Quality Assurance Program, Wyndham Hotels shall conduct periodic inspections to evaluate each Wyndham-branded hotel's establishment, implementation, and maintenance of its comprehensive information security program no less than every two years. Such inspections shall, at a minimum, be done in a manner comparable to the manner in which Wyndham Hotels evaluates a Wyndham-branded hotel's compliance with other Franchisor Standards covered by the Quality Assurance Program, and shall utilize an objective compliance measurement instrument approved by the third-party professional retained pursuant to Part IV below.
- E. Wyndham Hotels shall address any instance of a Wyndham-branded hotel's failure to establish, implement, or maintain its comprehensive information security program that becomes known to it through such Quality Assurance Program inspections or otherwise by directing such Wyndham-branded hotel to correct such failure within a reasonable time and by taking reasonable measures to address any deficiencies so as not to violate Part II of the order.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Parts II and III of this order, Wyndham Hotels shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) in the case of the initial Assessment, the first three hundred sixty-five (365) days after service

of the order; and (2) in the case of the ensuing biennial Assessments, each two (2) year period after the period covered by the initial Assessment, for twenty (20) years after service of the order. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondents, directly or indirectly, have implemented and maintained during the reporting period for Wyndham Hotels;
- B. explain how such safeguards are appropriate to Wyndham Hotels' size and complexity, the nature and scope of its activities, and the sensitivity of the personal information that is collected by it from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order;
- D. certify that the comprehensive information security program for Wyndham Hotels is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period; and
- E. certify that Wyndham Hotels has reasonably complied with Part III of this order during the reporting period in question.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Wyndham Hotels shall provide its initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Wyndham Hotels until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission in writing, the initial Assessment, and any subsequent Assessments requested, shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin *In the Matter of Wyndham Worldwide Corp., et. al.*, FTC File No. 1023142.

V.

IT IS FURTHER ORDERED that respondents shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. for a period of three (3) years after the date of preparation of each Assessment

required under Part IV of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondents, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Wyndham Hotels' compliance with Parts II, III, and IV of this order, for the compliance period covered by such Assessment;

- B. unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:
1. all advertisements and promotional materials containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation; and
 2. any documents, whether prepared by or on behalf of respondents, that contradict, qualify, or call into question respondents' compliance with this order.

VI.

IT IS FURTHER ORDERED that respondents shall deliver a copy of this order to all current and future subsidiaries, current and future Wyndham-branded hotels, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondents shall deliver this order to such current subsidiaries, Wyndham-branded hotels, and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after respondents acquire the subsidiary or the person assumes such position or responsibilities. For any future Wyndham-branded hotel, delivery shall be at least ten (10) days prior to respondents entering into a franchise or management agreement.

VII.

IT IS FURTHER ORDERED that respondents shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondents learn fewer than thirty (30) days prior to the date such action is to take place, respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In the Matter of Wyndham Worldwide Corp. et. al.*, FTC File No. 1023142.

VIII.

IT IS FURTHER ORDERED that respondents within one hundred eighty (180) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit an additional true and accurate written report.

IX.

IT IS FURTHER ORDERED that, so long as Wyndham Worldwide Corporation directly or indirectly holds The Hotel Group, Wyndham Hotels, or Hotel Management as a subsidiary, it shall ensure that they comply with this order. In the event Wyndham Worldwide Corporation no longer directly or indirectly holds The Hotel Group, Wyndham Hotels, or Hotel Management as a subsidiary, its obligations as to that entity under this Order shall cease immediately.

X.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondents did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

WYNDHAM WORLDWIDE CORPORATION

Dated: _____
By: _____
Wyndham Worldwide Corporation

WYNDHAM HOTEL GROUP, LLC

Dated: _____
By: _____
Wyndham Hotel Group, LLC

WYNDHAM HOTELS AND RESORTS, LLC

Dated: _____
By: _____

Wyndham Hotels and Resorts, LLC

WYNDHAM HOTEL MANAGEMENT, INC.

Dated: _____

By: _____
Wyndham Hotel Management, Inc.

Dated: _____

By: _____
DOUGLAS H. MEAL
Ropes & Gray LLP
One International Place
Boston, MA 02110-2624
Attorney for Respondents

Dated: _____

By: _____
LYDIA PARNES
Wilson Sonsini Goodrich & Rosati
1700 K St., N.W.
Washington, DC 20006
Attorney for Respondents

Dated: _____

By: _____
SETH SILBER
Wilson Sonsini Goodrich & Rosati
1700 K St., N.W.
Washington, DC 20006
Attorney for Respondents

Dated: _____

By: _____

KRISTIN KRAUSE COHEN
LISA WEINTRAUB SCHIFFERLE
Counsel for the Federal Trade Commission

APPROVED:

MARK EICHORN
Assistant Director
Division of Privacy and Identity Protection

MANEESHA MITHAL
Associate Director
Division of Privacy and Identity Protection

DAVID C. VLADECK
Director
Bureau of Consumer Protection

EXHIBIT 7- Redacted

EXHIBIT 8

CERTIFICATION DECLARATION

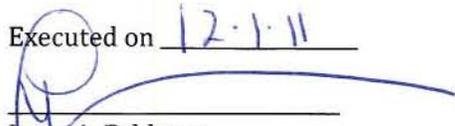
I am the general counsel of Wyndham Hotel Group, LLC. In that capacity, I oversaw (directly or indirectly through other company personnel under my supervision with respect to this matter or through outside counsel) the preparation of the written responses (the "Responses") and the document productions (the "Productions") that Wyndham Hotels & Resorts, LLC ("WHR"), a wholly-owned subsidiary of Wyndham Hotel Group, LLC, has made to the access letter dated April 8, 2010 (the "Access Letter") that was sent to WHR by the Federal Trade Commission (the "Commission"). A list of each of the Responses and each of the Productions is attached hereto as Schedule I.

The Productions included documents that WHR identified as being both non-privileged and responsive to one or more of the Access Letter's requests after conducting what WHR considered to be a reasonable search of certain document locations and a reasonable review of those documents located by the search. The document search targeted (1) certain specified data sources that WHR believed to be reasonably likely to contain documents responsive to Requests 1-4, 5(a)-(c), 5(e), 6-7 & 10-14 of the Access Letter (i.e., the requests calling for documents "sufficient" to identify certain information or otherwise requesting discrete categories of documents) (the "sufficient-to-show requests"); and (2) the reasonably accessible sources for electronically stored information with respect to which Jason Rowland and Mike Stevens were the custodians. To the best of my knowledge, information, and belief, after having made what I believe to have been a reasonable inquiry, the Productions included documents that satisfied the sufficient-to-show requests, except that in regard to Requests 10-11 WHR did not locate documents "sufficient to identify" the information sought by those requests. In regard to Requests 5(a), 8 & 9 (i.e., the Access Letter's "all documents" requests), to the best of my knowledge, information, and belief, after having made what I believe to have been a reasonable inquiry, in the aggregate the Productions included all documents that WHR located after making the above-described search and determined to both non-privileged and responsive to those requests after conducting the above-described review.

The Responses included information that WHR identified as being both non-privileged and responsive to one or more of the Access Letter's requests, and/or one or more follow-on requests by the Commission staff, after making what WHR considered to be a reasonable effort to locate such information. To the best of my knowledge, information, and belief, after having made what I believe to have been a reasonable inquiry, WHR intended for each Response to address fully and to provide all such information required by the requests that it referenced, and at the time each Response was made, WHR believed the statements in the Response to be accurate.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on 12-1-11



Lynn A. Feldman

WHR CERTIFICATION - SCHEDULE 1

WHR CERTIFICATION - SCHEDULE 1					
	Date	Description	Production Media	Bates Begin	Bates End
1	5/10/10	First Production	CD #1	WHR-FTC1000000001	WHR-FTC1000001521
2	6/10/10	Second Production	CD #2	WHR-FTC1000001522	WHR-FTC1000001744
3	7/19/10	First Response; Third Production	HD #1	WHR-FTC1000001745 WHR-FTC2000000001	WHR-FTC1000005343 WHR-FTC2000039006
4	9/8/10	Second Response	n/a	n/a	n/a
5	9/14/10	Fourth Production	CD #3	WHR-FTC1000005344	WHR-FTC1000008823
6	10/18/10	Third Response; Fifth Production	HD #2 HD #3	WHR-FTC1000008824 WHR-FTC2000039007 WHR-FTC2000559121	WHR-FTC1000009984 WHR-FTC2000559120 WHR-FTC2000951122
7	10/26/10	Sixth Production	CD #4	WHR-FTC2000951123	WHR-FTC2000983887
8	12/21/10	Seventh Production	CD #5	WHR-FTC2000983888	WHR-FTC2001000343
9	1/10/11	Fourth Response (updating first Response); Eighth Production	CD (not numbered)	WHR-FTC1000009985	WHR-FTC1000010007
10	5/27/11	Ninth Production	CD #6	WHR-FTC1000010008	WHR-FTC1000010120