THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

Federal Trade Commission, Plaintiff, v. Wyndham Worldwide Corporation, *et al.*, Defendants.	CIVIL ACTION NO. 2:13-CV-01887-ES-JAD **STIPULATED ORDER FOR INJUNCTION**

Plaintiff, the Federal Trade Commission ("Commission"), filed its Complaint for Injunctive and Other Equitable Relief, , ("FTC Act"), 15 U.S.C. § 53(b). The Commission and Defendants stipu

Stipulated Order for Injunction ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint alleges that Defendants participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, related to their data security.
3. The agreement contained in this Order is for settlement purposes only.
4. This Order does not constitute an admission by Defendants that the law has been violated as alleged in the complaint, or that the facts as alleged in the complaint, other than the jurisdictional facts, are true.

4. "Cardholder Data Environment" shall have the meaning PCI DSS Version 3.1, attached hereto as Appendix A, gives to the term "cardholder data environment," i.e., the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.
5. "Defendants" shall mean (1) Hotels and Resorts; (2) Wyndham Hotel Management, Inc.; (3) Wyndham Hotel Group, LLC and its successors and assigns; and (4) Wyndham Worldwide Corporation and its successors and assigns.
6. "Hotels and Resorts" shall mean Wyndham Hotels and Resorts, LLC, its subsidiaries and divisions, and its successors and assigns; provided, however, that in no event shall "Hotels and Resorts" include any of the Wyndham-branded Hotels. No entity shall be considered a subsidiary or a division for purposes of the definition of Hotels and Resorts in the event such entity is no longer a subsidiary or division of Hotels and Resorts.
7. "PCI DSS" shall mean the Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, Version 3.1, attached hereto as Appendix A, or, in the event such standard no longer exists, any successor standard established or approved by the Payment Card Industry Security Standards Council, any successor entity to said Council, or all of the major payment card brands. In the event no such successor standard or successor entity exists, PCI DSS shall mean a standard of comparable scope and thoroughness approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.
8. "Practice" shall mean any act or omission implicating information security, including any conduct, implementation, control, configuration, procedure, process, or policy.

9. "Treat as an untrusted network" shall mean to implement the security protections that PCI DSS Version 3.1, attached hereto as Appendix A, requires to be put in place with regard to an untrusted network.
10. "Untrusted network" shall have the meaning that Requirement 1.2 of PCI DSS Version 3.1, attached hereto as Appendix A, gives to the term "untrusted network," i.e., any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.
11. "Wyndham-branded Hotel" shall mean an independently-owned hotel that is operated in the United States pursuant to a management or franchise agreement with Hotels and Resorts or Wyndham Hotel Management, Inc. or any of their respective subsidiaries (a) under one of the following brand names or any successor brand name to one of the following brand names: Wyndham Hotels and Resorts, Wyndham Grand, and Wyndham Garden Hotels, or (b) under any other hotel brand name that is marketed by Hotels and Resorts to potential licensees of such brand name by means of a Franchise Disclosure Document or any other regulatory disclosure document generally required by the Federal Trade Commission to be delivered to a potential licensee in connection with the sale of a franchise.

ORDER

I. COMPREHENSIVE INFORMATION SECURITY PROGRAM

IT IS ORDERED that Hotels and Resorts shall, no later than the date of entry of this

be fully documented in writing, shall consist of the following administrative, technical, and physical safeguards appropriate to Hotels and Resorts' size and complexity, the nature and scope of Hotels and Resorts' activities, and the sensitivity of the Cardholder Data at issue:

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 Cardholder Data 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, (3) risks emanating from the Wyndham-branded Hotels, and (4) 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 (including any risks emanating from the Wyndham-branded Hotels), 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 Cardholder Data they receive from Hotels

and Resorts and requiring such service providers by contract to implement and maintain appropriate safeguards for such information; and

E. the evaluation and adjustment of Hotels and Resorts' information security program described herein in light of the results of the testing and monitoring required by Part I.C or any other circumstances (including any material changes to Hotels and Resorts' operations or business arrangements) that Hotels and Resorts knows or has reason to know may have a material impact on the effectiveness of such information security program.

II. CARDHOLDER DATA ASSESSMENTS

IT IS FURTHER ORDERED that, Hotels and Resorts shall, so long as there is a Cardholder Data Environment within a network that, as to Hotels and Resorts, is not an untrusted

is not treated as untrusted, certify that such network either is included in the Assessment or has during the 12 months preceding the Assessment separately been validated to be fully compliant with the Approved Standard;

2. certify as to the extent of Hotels and Resorts' compliance with each element of a risk management protocol at least as thorough as Version 2.0 of the PCI DSS Risk Assessment Guidelines, attached hereto as Appendix B; and

3. certify that the Assessment was conducted by a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession, adheres to professional and business ethics, performs all duties objectively, and is free from any conflicts of interest that might compromise the assessor's independent judgment in performing Assessments. Professionals qualified to prepare Assessments shall be: a person qualified as a Certified Information Systems 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; a Qualified Security Assessor under PCI DSS (QSA); or, at the election of Hotels and Resorts, a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

B. If the assessor that conducts an Assessment described in Part II.A does not certify that Hotels and Resorts is fully compliant with the Approved Standard on which the Assessment in question is based and with the risk protocol referenced in

the date of that Assessment or until the next December 31 Assessment deadline, whichever is earlier. *Provided, however*:

1. A Practice by Hotels and Resorts shall not be deemed in compliance with Part I of this Order based upon a Part II.A Assessment if Hotels and Resorts made a representation, express or implied, regarding the Practice that either misrepresented or omitted a material fact and such misrepresentation or omission would likely affect a reasonable Assessor's decision about whether the Practice complied with the Approved Standard. Further, in the event that such a misrepresentation or omission was made for the purpose of deceiving the assessor, Hotels and Resorts shall not be deemed compliant with any portion of Part I or Part II.A of this Order based on that Assessment.
2. Hotels and Resorts shall not be deemed in compliance with Part I of this Order based upon a Part II.A Assessment as to any Practice that is a significant change from any Practice in place at the time of the Assessment in question, unless, at the time of the significant change, an assessor qualified under Part II.A.3 certifies that the significant change does not cause Hotels and Resorts to fall out of compliance with the Approved Standard on which the Assessment in question was based.

This Court shall have exclusive jurisdiction over the construction of this Order in any matter or proceeding involving or relating to unfair data security practices for Cardholder Data. Hotels and Resorts shall provide each Assessment required by this Part II, including any Part II.B certification or Part II.C report, to the Associate Director for Enforcement, Bureau of Consumer

Compliance Reporting. Delivery must occur within fourteen (14) days of entry of this Order for current personnel. For all other personnel, delivery must occur before they assume their responsibilities.

IV. COMPLIANCE REPORTING

(a) any designated point of contact; or (b) the structure of that Defendant or any entity that that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, assignment, sale, merger, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any act or practice subject to this Order.

C. Unless otherwise directed by a representative of the Commission in writing, all submissions to the Commission pursuant to this Order 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: *FTC v. Wyndham Worldwide Corp., et al.*, FTC File No. X120032.

V. RECORDKEEPING

IT IS FURTHER ORDERED that Wyndham Worldwide Corporation, Wyndham Hotel

VI. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for purpose of monitoring Wyndham Worldwide Corporation's, Wyndham Hotel Group, LLC's, and Hotels and Resorts' compliance with this Order:

A. The Commission is authorized to seek discovery, without further leave of Court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69. Defendants may assert any and all objections, defenses, rights, or privileges in the Federal Rules of Civil Procedure, the Federal Rules of Evidence, or any other applicable law, as to any such discovery request.

B. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1. Defendants may assert any and all objections, defenses, rights, or privileges available to them, as to any such process.

C. This Part shall apply so long as Defendants are subject to any obligation in Part I or II of this Order, and for three years thereafter.

VII. WYNDHAM WORLDWIDE CORPORATION AND WYNDHAM HOTEL GROUP, LLC

IT IS FURTHER ORDERED that, so long as Wyndham Worldwide Corporation or Wyndham Hotel Group, LLC directly or indirectly holds Hotels and Resorts as a subsidiary, but in any event no longer than 20 years after entry of this Order, it shall ensure that Hotels and Resorts complies with this Order. In the event Wyndham Worldwide Corporation or Wyndham Hotel Group, LLC no longer directly or indirectly holds Hotels and Resorts as a subsidiary, but in any event no later than 20 years after entry of this Order, the obligations of Wyndham

Worldwide Corporation and Wyndham Hotel Group, LLC under this Order shall cease immediately.

VIII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall and does retain jurisdiction of this matter for purposes of, and shall have exclusive jurisdiction over, any matter or proceeding involving or relating to the modification and/or enforcement of this Order.

.

SO ORDERED this ___ day of _____, 201_.

_____
Hon. Esther Salas, U.S.D.J.

SO STIPULATED AND AGREED:

FOR FEDERAL TRADE COMMISSION:

Date: 12/8/15

Kevin H. Moriarty (DC Bar No. 975904)
Katherine E. McCarron (DC Bar No. 486335)
Jessica M. Rich (DC Bar No. 550732)
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

FOR DEFENDANTS:

Date:

Eugene F. Assaf (DC Bar No. 449778)
655 Fifteenth Street, N.W.
Washington, DC 20008
Tel: (202) 879-5196
Fax: (202) 879-5200
Email: eugene.assaf@kirkland.com

Attorneys for Defendants Wyndham Hotels and Resorts, LLC and Wyndham Hotel Management, Inc.

DEFENDANTS:

Date:

Wyndham Worldwide Corporation

Date:

Wyndham Hotel Management, Inc.

FOR DEFENDANTS:

[address]
[phone #]
[fax #]
[email]

n Worldwide Corporation, Wyndham Hotel Group, LLC,

Attorneys for Defendants Wyndha

FOR DEFENDANTS:

Date: _____

[address]
[phone #]
[fax #]
[email]