



ROPES & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPESGRAY.COM



ORIGINAL

PUBLIC

April 20, 2012

Douglas H. Meal
T +1 617 951 7517
F +1 617 235 0232
douglas.meal@ropesgray.com

BY HAND

Donald S. Clark
Secretary
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: Petition of Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation to Quash, or Alternatively, Limit Civil Investigative Demand, File No. 1023142

Dear Secretary Clark:

Pursuant to 16 C.F.R. § 2.7(f), Wyndham Hotels and Resorts, LLC (“WHR”) and its parent company, Wyndham Worldwide Corporation (“WWC” and, jointly with WHR, “Wyndham”), request a review by the full Federal Trade Commission (the “Commission” or “FTC”) of their Petition to Quash, or, Alternatively, Limit the Civil Investigative Demand (“Petition”) filed with the Commission on January 20, 2012. A copy of the Petition and its accompanying exhibits is attached hereto as Exhibits A and B respectively.¹ For the reasons set forth therein and further detailed below, Wyndham respectfully requests that the full Commission reverse Commissioner Julie Brill’s April 11, 2012 letter ruling (the “Letter Ruling”), attached hereto at Exhibit C,² insofar as it denied in part the Petition.

¹ Wyndham has requested, and Staff agreed by e-mail, that Exhibit 7 of the Petition (attached hereto as Exhibit B.7) will be treated as confidential and not part of the public record. E-mail from Lisa Schifferle, Federal Trade Comm’n, to Douglas H. Meal, Ropes & Gray LLP (Jan. 26, 2012, 4:47 pm EST). Pursuant to 16 C.F.R. § 4.2(d), Wyndham is filing herewith twelve copies of the request for review, twelve copies of the public exhibits, and twelve copies of the confidential Exhibit B.7. Also pursuant to § 4.2(d), Wyndham is enclosing a disc containing the request for review and all exhibits. Any questions regarding the confidentiality designation should be sent to the undersigned counsel of record.

² The Letter Ruling was served on counsel for Wyndham on April 17, 2012, so Wyndham’s request for full Commission review of the Petition is timely.

BACKGROUND³

For two full years, WHR has participated in a Commission investigation regarding its data security practices—an investigation that WHR has fully cooperated with throughout. The investigation was initiated by means of an access letter dated April 8, 2010 (the “Access Letter”), wherein the Commission advised WHR that the staff of the FTC (“Staff”) was conducting a non-public investigation into WHR’s compliance with federal laws governing information security (the “WHR Investigation”). According to the Access Letter, the WHR Investigation was prompted by the fact that, on three separate occasions since July 2008, certain independently-owned hotels licensed by WHR to use the Wyndham name (“Wyndham-branded hotels”) had suffered criminal intrusions into their computer networks (the “Intrusions”) in the course of which customer payment card data being handled by the intruded-upon hotels may have been placed at risk of compromise. The Access Letter stated that the WHR Investigation sought to determine whether WHR’s information security practices complied with Section 5 of the Federal Trade Commission Act (“Section 5”), which according to the letter “prohibits deceptive or unfair acts or practices, including misrepresentations about security and unfair security practices that cause substantial injury to consumers.”

Since April 8, 2010, WHR has produced to Staff over one million pages of documents in response to the twenty-nine separate documents requests (including subparts) contained in the Access Letter and ensuing Staff communications. In addition, WHR submitted to Staff five separate detailed written narratives responding to the fifty-one separate questions (including subparts) posed in the Access Letter and ensuing Staff communications. Further, the Chief Financial Officer and the head of Information Security for WHR, and/or WHR’s inside and outside counsel, made seven separate in-person presentations to Staff in an effort to address various questions Staff had raised in the course of the WHR Investigation.

Nevertheless, even after having received full cooperation with the WHR Investigation and all the documents and information engendered by that cooperation, Staff served Wyndham with a Civil Investigative Demand (“CID”) on December 8, 2011. The CID is a classic “kitchen-sink” discovery request that takes no account whatever of Staff’s previous requests and WHR’s previous responses to those requests, and makes no effort whatever to avoid unduly burdening Wyndham in responding to the CID. Including subparts, the CID includes no fewer than *eighty-nine* further interrogatories and *thirty-eight* further document requests. Because of the sheer volume of these sweeping requests and other defects in the CID, and after its efforts to meet and confer regarding the CID were

³ The accuracy of the factual statements made in this request for review pertaining to the Commission’s investigation into WHR’s compliance with federal laws governing information security (the “WHR Investigation”) is attested to in the Supplemental Declaration of Douglas H. Meal (Exhibit E hereto).

rebuffed by Staff, Wyndham moved to quash or, alternatively, limit the CID on January 20, 2012. On April 17, 2012, Wyndham's counsel was served with a letter from Commissioner Brill, dated April 11, 2012, denying in large part the Petition.

The Letter Ruling's substantial denial of the Petition appears, unfortunately, to have been based, in part, on a substantial misapprehension of the history of the WHR Investigation. Indeed, many of the crucial statements in the Letter Ruling regarding that history are not only unsupported by any citation to factual authority in the Letter Ruling itself, but in fact are directly contradicted by the factual statements in the "Background" section of the Petition, the accuracy of which were attested to in the Declaration of Douglas H. Meal, attached as Exhibit 2 to the Petition, which declaration stands entirely uncontradicted in the record. Without unnecessarily restating the entirety of the uncontested factual information already provided to the Commission by means of the Petition, Wyndham corrects the most significant misstatements in the Letter Ruling as follows:

First, no consumer suffered any injury—let alone substantial injury as required for an unfairness claim under the Federal Trade Commission Act ("FTCA")—as a result of the Intrusions. The Letter Ruling asserts that the exposure of payment card information "can result in harms including identity theft, financial fraud, and the basic inconvenience of replacing stolen card numbers." Letter Ruling, Exhibit C hereto, at 2. This assertion is plainly incorrect. To begin with, nothing in the statement by Chairman Deborah Platt Majoras cited for this proposition by the Letter Ruling supports the Letter Ruling's claim that the compromise of payment card information can result in identity theft. Rather, Chairman Majoras's statement discusses the risks *generally* created by the compromise of consumer data. In actuality, as noted throughout the Petition, because payment card issuers protect their cardholders against suffering any financial injury by reason of their payment card data being compromised, data security breaches that (like the Intrusions) only put payment card data at risk of compromise do not cause, and cannot cause, any financial injury to consumers, even assuming payment card information is in fact stolen from the breached entity during the event. Moreover, courts have consistently rejected the notion that the "inconvenience" associated with replacing compromised or potentially compromised payment card information is a legally cognizable injury. *See, e.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 497 (Me. 2010) ("[I]t must be established that the time and effort expended constitute a legal injury rather than an inconvenience or annoyance."). Accordingly, the Letter Ruling is simply wrong to suggest that there was any consumer injury as a result of the Intrusions. Indeed, the Letter Ruling's conclusion to that effect is belied by the Staff's own proposed complaint ("Proposed Complaint"), which does not even include an unfairness-based Section 5 claim,

presumably because Staff recognizes that no consumer injury occurred here, even though the Letter Ruling does not acknowledge that indisputable fact.⁴

Further, the Letter Ruling incorrectly asserts that the WHR Investigation extends not just to the information security practices of WHR, but also to the information security practices at WWC and another Wyndham affiliate, Wyndham Hotel Group, LLC (“WHG”). The Letter Ruling takes this position even though the Access Letter *by its own express terms* was addressed to an official at *WHR*, was prompted by intrusions into *WHR*’s computer networks having potentially resulted in the personal information of the customers of Wyndham-branded hotels being stolen, and was initiated for the purpose of determining whether *WHR*’s information security practices comply with Section 5 of the FTCA. Notwithstanding the Access Letter’s express and unambiguous language on these points, the Letter Ruling argues that, because the Access Letter’s document and information requests later purported to define “Wyndham” “to include not only WHR but also ‘its parents, subsidiaries, affiliates, franchisees, hotels managed by franchisees that use the Wyndham trade name, and agents,’” Letter Ruling, Exhibit C hereto, at 2, the targets of the WHR Investigation actually always included all the entities so defined as “Wyndham,” and not just WHR. Such a reading of the Access Letter is refuted by the plain language of the Access Letter itself, which states that the Commission “is conducting a non-public investigation into *Wyndham Hotels and Resorts, LLC*’s (‘Wyndham’) compliance with federal laws governing information security.” Access Letter, Exhibit B.3 hereto, at 1 (emphasis added). Moreover, the Letter Ruling’s reading of the Access Letter is also inconsistent with the conduct of the WHR Investigation. Each and every response to the Access Letter made clear that such response was being provided *by WHR* in response to a request the Commission had directed *to WHR*. Moreover, as noted in the Petition, Staff has *never* notified WHR of any Commission action to authorize the WHR Investigation to be expanded to include the information security practices at any of WHR’s affiliates and/or service providers.⁵ Nor does the Letter Ruling provide any evidence of any such Commission action ever having been taken, even in secret. Accordingly, there is not a shred of record evidence to support the Letter Ruling’s conclusion that the scope of the WHR Investigation includes the information security practices at entities other than WHR

⁴ The Letter Ruling also makes several other misstatements regarding the nature of the Intrusions, including the statement that they were disclosed in early 2010, Letter Ruling, Exhibit C hereto, at 2. As Staff is well aware, upon discovering each Intrusion in the period between 2008 and 2010, WHR undertook to notify any customer whose payment card data was potentially compromised as a result of the Intrusion in question. Wyndham also disputes the statement that the Intrusions resulted in the information relating to more than 619,000 payment cards having been actually compromised.

⁵ Of course, the fact that Staff provided WHR with a draft proposed complaint listing WWC, WHG, and WHM as respondents (see Exhibit B.5 hereto) does not show that the WHR Investigation ever targeted WWC, WHG and WHM. Instead, it shows that Staff inappropriately sought to include as respondents in a draft complaint entities that Staff never investigated.

and the Wyndham-branded hotels; indeed, all the evidence in the record on this point is directly to the contrary.

The Letter Ruling also states that (1) the “staff identified deficiencies in the production, most notably that WHR produced a large number of completely irrelevant and nonresponsive materials,” which included “multiple copies of third party software licenses, in various languages; numerous magazines and newsletters not specific to WHR; and, human resources materials” (Letter Ruling, Exhibit C hereto, at 2, 9 n.39) and (2) “WHR also failed to produce information that was obviously relevant to the investigation, such as supporting documents and information referenced in forensic reports that the company did provide” (Letter Ruling, Exhibit C hereto, at 2). These statements are wrong. Staff has never suggested that the totality of WHR’s document production and its responses to Staff’s questions did not respond fully to the Access Letter’s requests, or included significant non-responsive documents or information, or was in any other way deficient. *See* Petition, Exhibit A hereto, at 6. On the contrary, once WHR substantially completed its response to the Access Letter, Staff posed a few discrete additional document and information requests to WHR, most of which went beyond the Access Letter’s requests, and all of which WHR promptly and fully responded to. *That was the end of the matter.* In other words, the reason why the Letter Ruling contains not a single citation to any Staff communication that leveled at WHR the accusations regarding WHR’s response to the Access Letter that are made in the Letter Ruling is because *no such Staff communication exists or ever occurred.*

Needless to say, had Staff identified particular documents that WHR failed to produce, WHR would have undertaken to produce them—just as WHR did on several occasions following completion of its production of electronically stored information (“ESI”), when Staff requested prior versions of policies or other discrete documents not within the scope of the Access Letter’s original requests. However, Staff never once raised with WHR any alleged failure to produce responsive documents of the sort described in the Letter Ruling. And the Letter Ruling itself does not point with any specificity to any responsive document that WHR supposedly failed to produce. Based on the factual record, then, WHR’s Certification regarding the completeness of its response to the Access Letter (*see* Exhibit B.8 hereto) stands wholly un rebutted—meaning that the Letter Ruling’s finding of a failure by WHR to produce “information that was obviously relevant to the investigation” stands wholly unsupported.

Similarly, had Staff pointed WHR to those documents produced by WHR that Staff considered to be “irrelevant,” WHR would have been able to show Staff how the documents, “irrelevant” or not, were nonetheless responsive to one or more of the Access Letter’s requests. In so doing, WHR would have reminded Staff of how Staff had absolutely insisted that WHR do an ESI review in order to locate documents responsive to the Access Letter, even after WHR cautioned Staff that forcing such a review on WHR

would inevitably result in Staff's receipt of numerous documents that would be wholly irrelevant to the WHR Investigation, but nonetheless would be technically responsive to the Access Letter's requests.

Of course, the Letter Ruling provides no details regarding the "irrelevant" documents that WHR supposedly produced, so WHR can only speculate regarding the specific documents that the Letter Ruling characterizes as being "irrelevant." Suffice it to say that the documents produced by WHR were all (or at least nearly all⁶) *responsive* to one or more of the Access Letter's requests, so if many of those documents turned out to be "irrelevant" in Staff's judgment, that just goes to show how grossly overbroad the Access Letter's requests were in the first place (and, correspondingly, how grossly overbroad the CID's similarly worded requests are today). WHR's hunch is that the production of what the Letter Ruling describes as "a large number of completely irrelevant and nonresponsive materials" occurred as a result of the Staff's insistence that WHR produce all documents attached to or attaching an otherwise responsive document. If that is in fact what happened, the Letter Ruling should be pointing a finger at Staff for requesting these irrelevant documents, not at WHR for having produced them at Staff's request.

The Letter Ruling also misstates the sequence of events that led to settlement negotiations between WHR and the Staff. Contrary to the Letter Ruling, Staff, not WHR, first expressed an interest in pursuing settlement. Petition, Exhibit A hereto, at 8. Moreover, the Letter Ruling incorrectly states that WHR stated "that it could not respond to the Access Letter and negotiate settlement simultaneously." Letter Ruling, Exhibit C hereto, at 2. What actually occurred was that WHR and Staff agreed to put off, during the pendency of the parties' settlement negotiations, resolving Staff's request that WHR supplement its response to the Access Letter in two (and only two) ways: by (1) reviewing the ESI of additional custodians for documents responsive to the Access Letter's "all documents" requests and (2) advising Staff of any disagreements WHR had with the findings and conclusions contained in the forensic reports regarding the first and second Intrusions that were prepared on behalf of the card brands. There was no wholesale discontinuance, once settlement negotiations began, of WHR's efforts to cooperate with the WHR Investigation. To the contrary, even though WHR felt it had already responded fully to the Access Letter, and notwithstanding the fact that any investigation that has reached a point at which Staff has made a determination that the evidence adduced in the investigation created reason to believe that the target of the investigation has information security practices that violated Section 5 is by definition "complete," throughout the period

⁶ Until Staff identifies the exact documents to which the Letter Ruling was referring, Wyndham cannot exclude the possibility that they were produced through inadvertent human error. The fact remains, however, that Wyndham intended only to produce documents that were responsive to the Access Letter's requests or contained in a family of a document that was.

of settlement negotiations, WHR continued responding to information requests from Staff. *See* Petition, Exhibit A hereto, at 4-6.

The Letter Ruling also inaccurately implies that settlement discussions ceased on September 19, 2011 when “WHR informed staff it would not enter into a settlement on the terms Staff proposed.” Letter Ruling, Exhibit C hereto, at 3. As detailed in the Petition, what actually happened is that, in September 2011, WHR requested a meeting with Bureau of Consumer Protection (“BCP”) management to discuss WHR’s objections to the unlawful settlement terms being demanded by Staff. Thereafter, on November 21, 2011, in anticipation of the upcoming meeting with BCP Management, WHR submitted to BCP management a white paper detailing WHR’s objections to Staff’s settlement demands and the basis therefore. The meeting with BCP management did not occur, however, until December 15, 2011—seven days *after* the CID was issued. Thus, at the time the CID was issued, far from settlement negotiations having already failed, the parties were still in the midst of those negotiations. That being the case, there is every reason to believe, based on the timing of the CID’s issuance, that the purpose of the CID was indeed to gain leverage in the parties’ settlement negotiations, as Wyndham contends, and not to achieve any legitimate investigatory objective.

Finally, the Letter Ruling misstates what Staff had told WHR, prior to issuing the CID, regarding the information Staff felt it needed to complete the WHR Investigation. Letter Ruling, Exhibit C hereto, at 3. As noted in the Petition, prior to issuing the CID Staff, had advised WHR that Staff felt it needed (and accordingly would seek by CID) certain, limited additional information in order to complete its investigation. Petition, Exhibit A hereto, at 10. As noted above, according to Staff, this additional information was limited to two discrete tasks: (1) reviewing the ESI of additional custodians for documents responsive to the Access Letter’s “all documents” requests and (2) advising Staff of any disagreements WHR had with the findings and conclusions contained in the forensic reports regarding the first and second Intrusions that were prepared on behalf of the card brands. Accordingly, while WHR knew a CID was coming from Staff and hence was not surprised to receive one, WHR *was* completely surprised by the incredible breadth of the requests contained in the CID, which represented a complete about-face from what Staff had up to that point led WHR to believe would be sought by means of the CID.

ARGUMENT

As shown in the Petition, and as further described below, the CID is fundamentally flawed and should be quashed in its entirety or, at the very least, significantly limited.

First, as shown in the Petition, the issuance of a CID was not a valid exercise of the Commission’s statutory authority, because the CID was not authorized by a valid investigational resolution adopted by the Commission in the matter under investigation.

The Letter Ruling does not address this defect at all, instead focusing solely on the entirely separate question of whether the CID provides adequate notice of the nature and scope of the WHR Investigation. *See* Part I.A below. Next, the Petition showed that the CID was not issued based on the requisite showing that compulsory process is *needed* to advance the WHR Investigation. Here again, the Letter Ruling fails to address this particular defect in the CID. *See* Part I.B below. Moreover, even if the CID had been predicated on an investigational resolution of the sort required for compulsory process to be used in an FTC investigation, and even if the Commission could establish a necessity for such process to be used in the WHR Investigation, the CID does not provide the statutorily required notice of the purpose and scope of the WHR Investigation or of the nature of the conduct constituting WHR's alleged violation of Section 5 of the FTCA or of how Section 5 allegedly applies to WHR's conduct. *See* Part I.C below. Additionally, the Petition showed that the CID was issued for the improper purpose of either coercing WHR's acceptance of unlawful settlement terms or engaging in premature litigation discovery. The Letter Ruling disregards the facts set forth in the Petition demonstrating these improper purposes (all of which facts are undisputed in the record), and instead defends the propriety of the CID based on a fundamental misunderstanding of the factual background of the WHR Investigation, which misunderstanding not only has no evidentiary support in the record, but also is directly contradicted by the sworn declarations that the Commission has before it. *See* Part I.D below. Finally, the CID is invalid insofar as it seeks information and documents relative to the information security practices at WHR's affiliates and service providers, because the Access Letter expressly confirms that the investigation that the Staff was authorized to conduct involves only *WHR's* information security practices and *WHR's* compliance with Section 5—and not the information security practices or compliance with Section 5 at WHR's affiliates or service providers. *See* Part I.E below. For all the above reasons, the CID should be quashed as invalid.

Second, the CID is overly broad, unduly burdensome, and indefinite. As shown in the Petition and further detailed below, the CID is overbroad because it seeks numerous categories of information not reasonably related to the WHR Investigation, and the Letter Ruling does not offer an adequate justification for the CID's proposed fishing expedition into those categories. *See* Part II.A below. Next, contrary to the statements in the Letter Ruling, WHR and WWC more than adequately demonstrated the undue burden that compliance with the CID would impose. *See* Part II.B below. Finally, the CID is indefinite. The Letter Ruling deals summarily with this topic, and therefore does not address the fact that many of the CID's requests were not drafted so as to permit the requested material to be fairly identified by Wyndham. *See* Part III.C below. For these reasons as well, then, the CID should be quashed in its entirety by the full Commission or, at the very least, significantly limited.

I. THE CID IS INVALID**A. The Letter Ruling Misunderstands, and as a Consequence Overlooks, Wyndham's Argument that the CID Is Not Predicated on a Proper Investigational Resolution**

First and foremost, the Letter Ruling should be set aside because it misunderstands, and as a consequence overlooks, the leading argument in the Petition: namely, that regardless of what notice the CID provided or Wyndham otherwise had of the scope of the WHR Investigation, the CID is not predicated on a proper investigational resolution. Petition, Exhibit A hereto, at 16-20. Specifically, Wyndham showed in the Petition that a so-called "blanket" FTC resolution (such as the blanket January 2008 resolution ("January 2008 Resolution")) relied upon by Staff to issue the CID) cannot satisfy the statutory and regulatory requirement that a CID be issued pursuant to a valid Commission resolution (the "investigational resolution requirement"), as such a reading would contradict the text and purpose of the relevant statute and regulations. *See* Petition, Exhibit A hereto, at 17-18. Alternatively, the Petition showed that even if the investigational resolution requirement could theoretically be satisfied in a given case by a "blanket" resolution, the January 2008 Resolution pertains by its own terms only to an unspecified investigation that existed in 2008 and thus cannot form the proper predicate for *this* CID, which undisputedly was issued not in the 2008 investigation that is the subject of the January 2008 Resolution, but rather in the entirely separate *WHR Investigation*, which began in 2010. Petition, Exhibit A hereto, at 18-20.

The Letter Ruling mistakenly characterizes Wyndham's above argument as a mere contention that the CID and the January 2008 Resolution "fail[ed] to inform [Wyndham] sufficiently of the nature and scope of the investigation." Letter Ruling, Exhibit C hereto, at 3. The Letter Ruling thus collapses into a single inquiry two separate requirements for a valid CID: (1) the *investigational resolution* requirement, i.e., the requirement that any CID be predicated on a valid investigational resolution, *see* 15 U.S.C. § 57b-1(i); 16 C.F.R. §§ 2.4, 2.7; and (2) the *notice* requirement, i.e., the requirement that a CID provide an adequate description of the purpose and scope of the investigation, the nature of the conduct constituting the alleged violation, and the applicable provisions of law, *see* 15 U.S.C. § 57b-1(c)(2); 16 C.F.R. § 2.6. The Letter Ruling's error in treating these two separate requirements as involving a single inquiry led the Letter Ruling to overlook the Petition's arguments regarding the investigational resolution requirement. Because those overlooked arguments are meritorious, the full Commission must set aside the Letter Ruling and quash the CID in its entirety.

The investigational resolution requirement is entirely distinct from, and cannot be satisfied merely by meeting, the notice requirement. Whereas the notice requirement ensures that the recipient of a CID, and just as important a reviewing court, are advised of

sufficient information regarding the investigation to enable them to evaluate the propriety of the requests contained in the CID, the investigational resolution requirement, by contrast, serves the entirely different purpose of ensuring that the full Commission, and not merely a single Commissioner or the Commission's staff, makes the important determination that the use of compulsory process is warranted in the particular investigation in question. *See* 16 C.F.R. § 2.4 (resolution authorizing compulsory process must issue in a "matter under investigation"); S. Rep. No. 96-500, at 1125, 27 (Commission must only use compulsory process where information is "not available through other means"). Given the different purposes served by the two requirements, no amount of information regarding the investigation in question that might be provided in satisfaction of the notice requirement—whether that information is included within the CID itself, in a resolution or other document attached to the CID, or within communications between the Staff and the CID recipient during the course of the investigation—can ever satisfy the investigational resolution requirement, because *that* requirement turns on whether the full Commission adopted, and had a proper basis for adopting, a resolution in the matter under investigation authorizing the use of compulsory process in *that* investigation.

Because the Letter Ruling erroneously collapses its analysis of the investigational resolution requirement into an assessment of the adequacy of the notice of the investigation provided by the CID, the cases the Letter Ruling cites in support of its analysis are entirely irrelevant to Wyndham's argument that the investigational resolution requirement was not met here. Every single case cited by the Letter Ruling in support of its conclusion that the investigational resolution requirement was satisfied here addresses only the notice requirement⁷ or, in one case, addresses only the separate requirement that any information sought by the CID be relevant to the investigation (which requirement is discussed at II.A, *infra*).⁸ *See* Letter Ruling, Exhibit C hereto, at 3-6. Moreover, not a single case cited in

⁷ *See FTC v. O'Connell Assocs.*, 828 F. Supp. 165, 170-71 (E.D.N.Y. 1993) (assessing adequacy of a CID's notice under FTCA Section 20(c)(2), 15 U.S.C. § 57b-1(c)(2)); *FTC v. Carter*, 636 F.2d 781, 787 (D.C. Cir. 1980) (rejecting the argument that the resolution "fails to provide adequate notice of the purposes of the investigation"); *FTC v. National Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (rejecting an argument that the FTC's "statement of scope and nature" of the investigation was sufficient under 16 C.F.R § 2.6, "Notification of Purpose"); *Assocs. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) (rejecting the argument that an omnibus CID failed to meet the notice requirement of Section 20(c)(2), in part because notice was given through means—correspondence, e.g.—other than the CID and accompanying resolutions); *Dr. William V. Judy*, No. X000069, at 4-5 (Oct. 11, 2002) (rejecting the argument that an omnibus CID failed to meet the notice requirement of Section 20(c)(2)), available at <http://www.ftc.gov/os/quash/021011confirmanthonyltr.pdf>; *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010) (noting that "[t]he Commission is not required to identify to Petitioners the specific acts or practices under investigation"), available at <http://www.ftc.gov/os/quash/100712hortonresponse.pdf>.

⁸ *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992) (stating Commission has no "obligation to establish precisely the relevance of the material it seeks in an investigative subpoena by tying that material to a particular theory of violation").

the course of the Letter Ruling's analysis of the investigational resolution requirement involved a "blanket" resolution, the type relied upon by the Staff here. Instead, all involved either a "special" resolution, *Invention Submissions*, 965 F.2d 1086, 1087 (D.C. Cir. 1992), or an "omnibus" resolution directed at a specific industry.⁹ Nor is there any indication that the resolutions in these cases were not adopted in the very same pre-existing, ongoing investigation in which the CID in question was issued. By contrast, here the January 2008 Resolution was adopted as part of a completely *different* investigation than the investigation in which the CID issued. In short, the cases cited by the Letter Ruling offer no support for a conclusion that the CID issued was predicated on a Commission resolution that satisfied the investigational resolution requirement in regard to the CID.

The Letter Ruling's failure to appreciate that the investigational resolution requirement is distinct from the notice requirement no doubt explains why the Letter Ruling entirely overlooks the key pieces of authority cited by Wyndham in support of its analysis of the investigational resolution requirement's application to this particular case. Most importantly, as Wyndham argued in the Petition, both the legislative history of 15 U.S.C. § 57b-1(i) and the express language of 16 C.F.R. § 2.4, as well as the Commission's own Operating Manual¹⁰ require that any investigational resolution be issued *in a matter currently under investigation*, because that is the only way the Commission can evaluate whether the use of compulsory process is necessary in that particular investigation. 16 C.F.R. § 2.4 ("any matter under investigation"); Petition,

⁹ See *O'Connell Assocs.*, 828 F. Supp. at 167 n.1 (the consumer credit reporting industry); *Carter*, 636 F.2d at 784 (cigarette marketing); *National Claims Serv.*, 1999 WL 819640, at *2 ("business opportunity" industry); *Assocs. First Capital Corp.*, 127 F.T.C. 910, 911 (1999) (subprime lending); *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 2 n.2 (July 12, 2010) (loan marketing); *William V. Judy*, No. X000069, at 4-5 (Oct. 11, 2002) (dietary supplement marketing).

¹⁰ The Letter Ruling dismisses Wyndham's argument that the Commission's own Operating Manual contains persuasive statements that compellingly illustrate how the agency's power to issue CIDs is restricted by the statutory investigational resolution requirement in exactly the manner that Wyndham has argued (*see* Petition, Exhibit A hereto, at 16-20), by observing that the Operating Manual is not binding on the Commission and in any event is not enforceable against the Commission by Wyndham. To be clear, Wyndham does not and did not argue, as the Letter Ruling states (Letter Ruling, Exhibit C hereto, at 5 n.21), that the Operating Manual is binding on the Commission or enforceable by Wyndham. Wyndham merely argues that the Commission's own Operating Manual is persuasive authority as to the proper interpretation of the relevant statute and regulation—which *are* binding on the Commission and *are* enforceable against the Commission by Wyndham—and that Staff's failure to comply with the Operating Manual in seeking issuance of the CID here is persuasive evidence of the improper purpose that motivated Staff to seek issuance of the CID.

Exhibit A hereto, at 16-20.¹¹ Thus, “blanket” resolutions (here, the January 2008 Resolution) that nowhere even *mention*, and were issued before the commencement of, the particular investigation in which the CID was issued (here, the WHR Investigation) do not and cannot satisfy the investigational resolution requirement, because they represent an abdication of the Commission’s congressionally mandated responsibility to evaluate on a case-by-case basis the propriety of using compulsory process in Staff investigations. The Letter Ruling’s assertion that the law “does not require a separate investigational resolution for each investigation” (Letter Ruling, Exhibit C hereto, at 5)¹² is therefore simply wrong, at least in regard to investigational resolutions that authorize the use of compulsory process. Indeed, the requirement that any such investigational resolution be adopted *in the matter under investigation* is made clear not only by the legislative history of 15 U.S.C. § 57b-1(i) that the Letter Ruling chooses to ignore,¹³ but also by the critical “in any matter under investigation” language expressly contained in the Commission’s own rule on the subject. The Letter Ruling thus not only fails to observe the canon of statutory construction calling for an act of Congress to be interpreted in accordance with Congress’s clearly expressed intent in enacting the provision, but also violates the elementary principle

¹¹ On January 13, 2012, the Commission proposed a new version of Rule 2.4 that omits from the rule the crucial language “in any matter under investigation.” 77 Fed. Reg. 3191, 3196 (Jan. 13, 2012). Plainly, this change is intended by the Commission to “fix” the “problem” (which problem had previously been raised by other companies targeted by CIDs issued under “blanket” FTC resolutions) that the Commission’s purported authority to rely on blanket resolutions in authorizing compulsory process is directly belied by the Commission’s own regulation on the subject. To say the least, it is disturbing that the Commission seeks by its proposed change to Rule 2.4 to delete regulatory language that honors Congress’s clear intent to restrict the circumstances under which compulsory process may issue in FTC investigations. Even more disturbing, the Commission’s section-by-section analysis of the proposed revision to Rule 2.4 makes no mention of this deletion and thus fails to draw this very significant change to the attention of the public and parties who may be affected by it. 77 Fed. Reg. at 3192 (Jan. 13, 2012). In any event, the current Rule 2.4, not the proposed Rule, governs the Petition, and the Commission’s defective public notice of the change embedded in the proposed Rule will prevent the Commission from taking any advantage of that change in future disputes of this sort.

¹² See also Letter Ruling, Exhibit C hereto, at 4 n.15 (“The issue of whether a resolution is blanket or omnibus is not relevant because either is an acceptable form of resolution.”); *Id.* at 5 (“[C]ontrary to Petitioners’ contention, the resolution is not invalid because it is a so-called ‘blanket resolution.’”); *Id.* (“[N]o such requirement arises under the Commission’s Rules.”).

¹³ Specifically, the Letter Ruling overlooks the legislative history cited by Wyndham demonstrating that the Commission’s use of broad, vague “blanket” resolutions as authority for compulsory process to be used in an FTC investigation cannot be squared with Congress’s clearly expressed goal of limiting the use of CIDs in such investigations to situations where information cannot be obtained voluntarily. Petition, Exhibit A hereto, at 18.

that a law should be interpreted so as not to render any of its phrases or provisions (here, the “in any matter under investigation” provision of 16 C.F.R. § 2.4) meaningless.¹⁴

In short, the Petition’s argument that the CID fails to meet the investigational resolution requirement stands wholly unrebutted by the Letter Ruling. That being the case, the full Commission should hold for the reasons stated in the Petition that the CID was not predicated on a valid investigational resolution and, as a result, should be quashed.

B. The Letter Ruling Does Not Address, and Hence Tacitly Concedes the Validity of, Wyndham’s Argument that the CID Was Not Issued Based on the Required Showing of Need for the Use of Compulsory Process

As described in the Petition, the FTCA prohibits the use of compulsory process in an FTC investigation unless the Commission’s staff adequately demonstrates, and the Commission validly finds, that such process is *needed* to advance that particular investigation. Petition, Exhibit A hereto, at 20-23. Specifically, the law is clear that where, as here, a company has already voluntarily provided substantial information during an investigation, Section 20(i) permits compulsory process to thereafter be used in that investigation only if (i) “the [C]ommission determines, after reviewing the initial submission, that more information is required,” and (ii) “the information is not available through other,” such as voluntary, means. Petition, Exhibit A hereto, at 21 (quoting S. REP. NO. 96-500, at 1127 (1979)). The Letter Ruling’s assertion that FTC Staff is not required to “show that the CID is necessary” (Letter Ruling, Exhibit C hereto, at 10) is thus simply incorrect as a matter of law.

Based on its mistaken reading of the applicable law, the Letter Ruling makes no attempt to refute (indeed, it nowhere mentions) Wyndham’s showing that, here, the Commission has failed to show that the documents and information sought by the CID could not be obtained voluntarily. Of course, any such attempt would have been unavailing, given that WHR has already voluntarily provided Staff with an enormous volume of information and documents requested by Staff, and given that Staff has never asserted to WHR that WHR’s voluntary production is in any way deficient or incomplete. Indeed, even now WHR stands ready to voluntarily make a further production of reasonable size and scope to Staff, further belying any claim by Staff that compulsory process is necessary in order to obtain such information. Accordingly, because Staff was required, but failed, to predicate issuance of the CID on a showing that the information

¹⁴ *Williams v. Taylor*, 529 U.S. 362, 404 (2000) (“It is . . . a cardinal principle of statutory construction that we must ‘give effect, if possible, to every clause and word of a statute.’” (quoting *United States v. Menasche*, 348 U.S. 528, 538-39 (1955))); *New York Currency Research Corp. v. CFTC*, 180 F.3d 83, 92 (2d Cir. 1999) (“Construing a regulation is similar to interpreting a statute Our first task is to ascertain the plain meaning . . .”).

sought thereby would not be provided voluntarily, the full Commission should for this reason alone quash the CID. *See* Petition, Exhibit A hereto, at 20-23.

C. The CID Does Not Contain the Statutorily Required Description of the Purpose and Scope of the WHR Investigation, the Nature of the Conduct Constituting WWC's and WHR's Alleged Section 5 Violation, and How Section 5 Allegedly Applies to WWC's and WHR's Alleged Conduct

The Petition established that the CID failed to sufficiently describe the nature of the conduct constituting the alleged violation under investigation and the applicable provision of law, as required by Section 20(c)(2) of the FTCA, as well as to state the purpose and scope of the investigation, as required by 16 C.F.R. § 2.6. The CID merely refers to the January 2008 Resolution for the "Subject of the Investigation," which resolution is inadequate to satisfy the notice requirements because such resolution does not even mention WHR, WWC, or any other Wyndham affiliate or service provider, let alone describe the conduct of any of these entities constituting the alleged violation, and does not describe how Section 5 of the FTCA is allegedly applicable to the conduct of any of such entities. *See* Petition, Exhibit A hereto, at 24-26.

The Letter Ruling asserts that the January 2008 Resolution "adequately delineates the purpose and scope of the investigation" because it refers generally to "deceptive or unfair acts or practices related to consumer privacy and/or data security" and that, therefore, "[t]here is no need to either state the purpose of an investigation with greater specificity, or tie the conduct under investigation to any particular theory of violation." Letter Ruling, Exhibit C hereto, at 4. It is hard to imagine how the January 2008 Resolution, which purports to apply to *any* person, partnership or corporation engaged in or affecting commerce and relates in any way to consumer privacy and/or data security, provides any principle that might limit or define the purpose and scope of the investigation. Not only does the January 2008 Resolution fail to reference WHR, but also it was issued prior to the first of the Intrusions and more than two years before the Staff commenced the WHR Investigation. The January 2008 Resolution thus in essence purports to be a blank check for compulsory process in connection with any alleged violation of Section 5 that relates in any way to consumer privacy and/or data security, authorizing just the type of abusive behavior that Congress sought to eliminate over 30 years ago. None of the cases

cited in the Letter Ruling approved of such indefinite, broad language.¹⁵ In each of the cited examples, the CID, at the very minimum, stated that the investigation was limited to a particular industry, if not a particular entity, and included reference either to a specific act or practice under investigation, *Invention Submission Corp.*, 965 F.2d at 1088; *Carter*, 636 F.2d at 788, or to a specific statutory and/or regulatory provision though to have been violated in addition to Section 5, *National Claims Serv., Inc.*, 1999 WL 819640 at *2; *O'Connell Assocs.*, 828 F. Supp at 171. The January 2008 Resolution contains no such limitations or descriptions.

The Letter Ruling also argues that, because Wyndham has produced documents and provided other information in response to the Access Letter, has received a proposed draft complaint, has engaged in settlement negotiations, and has prepared a white paper regarding its objections to the unlawful settlement terms being insisted upon by Staff, “the nature and scope of the investigation are quite clear to [Wyndham].” Letter Ruling, Exhibit C hereto, at 4. The Letter Ruling thus in essence suggests that the sole function of the notice requirement for a CID is to inform the *target* of the nature and scope of the investigation, such that the FTC is relieved from that statutory requirement when the target has already independently received the required notice. The Letter Ruling is wrong on this point. Because a CID is not self-executing, it may only be enforced by order of a district court. Accordingly, the statutory and regulatory requirements under which the CID *itself* must set forth the nature and scope of, and other information regarding, the investigation in which the CID is issued are intended to ensure not only that the target may gauge the relevancy to the investigation of the CID’s requests but also that a *reviewing court* has

¹⁵ See *National Claims Serv., Inc.*, 1999 WL 819640, at *2 (“the FTC stated the subject of investigation as unnamed business opportunity firms who sell ‘business opportunities ... to consumers [and] have been or are engaged in unfair or deceptive acts or practices in violation of 16 C.F.R. 436 and/or Section 5 of the Federal Trade Commission Act.’”); *O'Connell Assocs.*, 828 F. Supp. at 170-71 (CID referred to resolution authorizing compulsory process “[t]o determine whether unnamed consumer reporting agencies or others are or may be engaged in acts or practices in violation of Section 5 of the Federal Trade Commission Act ... and of the Fair Credit Reporting Act [FCRA].”); *Invention Submission Corp.*, 965 F.2d at 1088 (CID stated investigation’s purpose was “[t]o determine whether Invention Submission Corporation ... may be engaged in unfair or deceptive acts or practices ... including but not limited to false or misleading representations made in connection with the advertising, offering for sale and sale of its services relating to the promotion of inventions or ideas ... [and] to determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.”); *Carter*, 636 F.2d at 788 (“The Commission additionally defined the application of section 5 in the Resolution by relating it to the subject matter of the investigation ‘the advertising, promotion, offering for sale, sale, or distribution of cigarettes. . . .’”).

sufficient information upon which to make the relevancy evaluation.¹⁶ What WHR may or may not independently understand to be the nature and scope of the WHR Investigation will provide a reviewing court with no assistance whatever in reviewing the CID's propriety under Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice.¹⁷ Rather, a reviewing court will need to refer to the CID itself in conducting that review—an effort that would prove to be pointless here, given that the January 2008 Resolution referenced by the CID fails to mention or otherwise reference the WHR Investigation (let alone its purpose and scope), fails identify the target of such investigation (let alone the nature of the conduct constituting the alleged violation that is under investigation), and fails to describe how the provision of law cited therein is applicable to such conduct. Accordingly, there is literally nothing in the CID upon which a reviewing court could rely in order to determine that the CID is consistent with the statutory and regulatory requirements. This failing therefore requires that the CID be quashed in its entirety.

Moreover, Wyndham disputes the Letter Ruling's assertion that the prior history of the WHR Investigation somehow adequately notified WHR of the purpose and scope of the WHR Investigation. For example, there is nothing in the document production or other responses to information requests by Staff that would support the Staff's expansion of the investigation to include the information security practices at WWC, WHG, or WHM. Indeed, because the information technology assets of such entities were physically distinct and logically separated and because the forensic evidence shows no proof of such entities being impacted by the Intrusions, there is no basis for an allegation that customer data at any such entities was ever at risk of compromise in the Intrusions or that such entities ever suffered from information security deficiencies. Petition, Exhibit A hereto, at 4. WHR never received any documentation from Staff advising WHR that the WHR Investigation

¹⁶ See, e.g., *Texaco*, 555 F.2d at 874 (“The relevance of the material sought by the FTC must be measured against the scope and purpose of the FTC’s investigation, *as set forth in the Commission’s resolution.*”) (emphasis added); cf. S. Rep. No. 96-500 at 1125 (“The adoption of this provision is intended to limit the practice of the Commission of giving a vague description of the general subject matter of the inquiry *and provides a standard by which relevance may be determined.*”) (emphasis added); Operating Manual § 3.3.6.7.4.1 (“Investigational resolutions must adequately set forth the nature and scope of the investigation. The statement may be brief, but it must be specific enough *to enable a court in an enforcement action to determine whether the investigation is within the authority of the Commission and the material demanded by the compulsory process is within the scope of the resolution.*”) (emphasis added).

¹⁷ Indeed, nothing in the statutory or regulatory framework, legislative history, or case law (including the cases cited in the Letter Ruling) support the proposition that communications and prior dealings between the parties may be used to correct an otherwise deficient notice. Indeed, just as the target of an investigation cannot rely upon statements by the Staff to support a narrower interpretation of the scope of the investigation, see *FTC v. Invention Submission Corp.*, 1991 WL 47104, *2 (D.D.C 1991), *aff’d* 965 F.2d 1086 (D.C. Cir. 1992) (“[w]hen a conflict exists in the parties’ understanding of the purpose of an agency investigation, *the language of the agency’s resolution must govern.*”) (emphasis added), the Commission is similarly restricted from relying upon such understanding to support its interpretation of the language of the CID or otherwise to correct a deficient notice.

had been expanded to the information security practices at such entities, and neither WWC nor any other WHR affiliate ever received any documentation notifying such entity that the information security practices regarding personal information collected by such entity *itself* had become a target of the WHR Investigation. Petition, Exhibit A hereto, at 30. Thus, even if the Letter Ruling were correct that the FTC need not set forth in the CID itself the statutorily required information regarding the investigation in which the CID is issued where the target of the investigation is independently aware of that information, here Wyndham indisputably was not independently aware of that information, so the notice contained in the CID regarding the nature and scope of the WHR Investigation is deficient even under the Letter Ruling's theory. At a minimum, then, the CID should be quashed insofar as it seeks documents and information relating to the information security practices at any entity other than WHR or any Wyndham-branded hotel.

D. The Letter Ruling Fails To Address WHR's Evidence Demonstrating That The CID Was Issued for the Improper Purpose of Either Coercing WHR's Acceptance of Unlawful Settlement Terms or Engaging in Premature Litigation Discovery (or Both)

The Petition presented compelling evidence that the CID was issued for the improper purpose of either coercing WHR's acceptance of unlawful settlement terms or engaging in premature litigation discovery. Petition, Exhibit A hereto, at 26-28. The Letter Ruling disregards that evidence entirely—never mentioning it once. Instead, relying on a misunderstanding of the factual background of the WHR Investigation that is nowhere supported in the record and in fact is directly contradicted by the only sworn testimony contained in the record, the Letter Ruling finds that Staff acted with a proper purpose in seeking and obtaining issuance of the CID. The Letter Ruling's finding is unsustainable. Accordingly, the full Commission should quash the CID in its entirety.

According to the Letter Ruling, the Petition's compelling evidence that the CID was issued for an improper purpose (all of which evidence is left uncontested by the Letter Ruling and accordingly must be accepted as true by the Commission in its review of the Letter Ruling) is conclusively refuted by the following supposed "facts" (see Letter Ruling, Exhibit C hereto, at 12)—none of which is accurate:

1. ***"Mid-investigation, Petitioners expressed an interest in exploring settlement talks as a means of resolving the matter short of a full-blown investigation and consequent possible law enforcement action."*** That never happened. What really happened was that *Staff*, not WHR, expressed an interest in settlement so that Staff would not have to complete its investigation, which by that point was already "full-blown" by any standard, having cost WHR millions of dollars and having resulted in Staff's receipt of more than one million pages of documents and complete answers to all of its interrogatories.

2. ***“At Petitioners’ request, staff voluntarily allowed them to suspend their production, in order to reduce the burden on Petitioners.”*** That never happened. By the time Staff raised the possibility of settlement, WHR had already *completed* its production, at least as far as WHR was concerned. The only issue that remained on the table at that point regarding Staff’s investigation was Staff’s request (which WHR was prepared to negotiate) that WHR supplement its response to the Access Letter in two (and only two) ways: by (1) reviewing the ESI of additional custodians for documents responsive to the Access Letter’s “all documents” requests and (2) advising Staff of any disagreements WHR had with the findings and conclusions contained in the forensic reports regarding the first and second Intrusions that were prepared on behalf of the card brands. Staff and WHR agreed to table that issue—and *only that issue*—during the pendency of the parties’ settlement negotiations. Thus, throughout the parties’ settlement negotiations, Staff continued to request, and WHR continued to comply with, other requests Staff made for discrete documents and pieces of information that had not been included in WHR’s original response to the Access Letter (almost always because they were not called for by the Access Letter’s requests).

3. ***“But staff also advised Petitioners that they would resume their investigation should settlement talks fail.”*** That never happened. What really happened was that Staff advised WHR that should settlement talks fail, Staff reserved the right at that point to renew its request that WHR supplement its response to the Access Letter in the two ways set forth above—and only in those two ways. Prior to WHR’s rejection of Staff’s unlawful settlement terms in September 2011 and WHR’s simultaneous request for an opportunity to meet with BCP management in order to present its objections to those unlawful terms, Staff *never* claimed that WHR’s response to the Access Letter had been incomplete in any significant way; Staff *never* asserted that WHR’s document production in response to the Access Letter included numerous non-responsive documents; Staff *never* indicated that it intended to request any additional information from WHR beyond the two categories that had been tabled during the parties’ settlement negotiations; and Staff *never* said it planned to try to obtain such additional information by means of a CID, rather than through the voluntary process it had been successfully employing up to that point.

4. ***“And, as Petitioners admit, when the CID was issued, it was no surprise.”*** Wyndham has admitted no such thing. To be sure, in October 2011, shortly after WHR advised Staff that WHR would not accede to Staff’s unlawful settlement demands and requested a meeting with BCP management to present its objections to those demands, Staff advised WHR *for the first time* that Staff intended to serve Wyndham with a CID in order to seek the information Staff believed it needed to complete the WHR Investigation. Having been so advised by Staff in October, WHR was not surprised to receive a CID in December. WHR *was* surprised, however, that instead of merely seeking just the two categories of information that had been tabled during the parties’ settlement negotiations,

the CID sought a welter of information that Staff had no legitimate basis for seeking and that Staff had never once previously expressed an interest in getting.

Because the “facts” that the Letter Ruling relies upon to refute Wyndham’s improper-purpose argument are not actually “facts” at all, that argument stands entirely unrebutted on the record before the full Commission. In particular, the Letter Ruling never challenges any of the following *actual facts*, which taken together compel the conclusion that the CID was indeed issued for the improper purpose of either coercing WHR’s acceptance of unlawful settlement terms or engaging in premature litigation discovery:

- The CID (i) pervasively duplicates Staff’s prior requests for documents and information made during the course of the WHR Investigation; (ii) is patently overbroad without authority seeking to expand the WHR Investigation at the eleventh hour to WHR’s affiliates and service providers; (iii) is wholly unnecessary given that the WHR Investigation has by Staff’s own admission already achieved its investigatory objective; and (iv) is unjustifiably burdensome when one takes into account the vast amount of information WHR has already provided to Staff at huge expense during the sixteen-month course of the WHR Investigation, the enormous costs Wyndham would incur in trying to comply with the CID, and the trivial nature of the Section 5 violation that Staff believes it found after sixteen months of investigating WHR’s information security practices. This combination of gross defects in the CID itself, coupled with the legally defective process by means of which Staff sought and obtained issuance of the CID (as discussed above in Parts I.A-I.C), makes it impossible to conclude that the CID has a genuine investigatory purpose, and instead suggests strongly that an improper purpose must underlie it.
- The CID was served on WHR only days after Staff received WHR’s white paper demonstrating the unlawfulness of the settlement terms being demanded by Staff and objected to by WHR. Tellingly, the Letter Ruling never once tries to defend the lawfulness of those settlement terms. The undisputed impropriety of the settlement terms being demanded by Staff certainly raises an inference that the purpose underlying the CID is likewise improper.
- WHR provided Staff with an opportunity to explain the purpose of the CID. Staff, however, declined and flatly refused Wyndham’s request for a copy of its internal memorandum requesting issuance of the CID, even though that memorandum is directly relevant to the Staff’s purpose in seeking issuance of the CID. Staff’s refusal to disclose this directly relevant

document as to its purpose in seeking the CID permits an adverse inference to be drawn regarding the propriety of that purpose.

- Moreover, Staff has provided WHR with no rebuttal of any sort to the arguments WHR advanced in the white paper as to the unlawfulness of the settlement terms being demanded by Staff. To this day—nearly five months after the white paper was delivered—Staff’s primary reaction to the legal arguments in WHR’s white paper has been to improperly seek and obtain issuance of the CID.
- Contrary to the Letter Ruling’s presentation, Staff issued the CID *in the midst of* settlement negotiations—not after those negotiations failed. Specifically, the CID was issued immediately prior to WHR’s scheduled meeting with BCP management for the purpose of presenting WHR’s objections to the unlawful settlement terms being demanded by Staff. This timing makes plain that the CID was designed to coerce WHR into accepting Staff’s unlawful settlement terms and to retaliate against WHR’s refusal to accept those terms earlier.
- By the time the CID was issued, Staff had already advised WHR that Staff believed, based on the results of the WHR Investigation, that WHR’s information security practices violated Section 5. Staff had further advised WHR that, based on that belief, Staff was ready to recommend that the Commission take corrective action against WHR. By the time the CID was issued, then, Staff plainly had no need for further discovery from WHR in order to complete the investigatory phase of the case and move forward with the corrective action phase.

The Letter Ruling tacitly concedes (certainly it does not dispute) that if Staff in fact did seek issuance of the CID for the purpose of either coercing WHR’s acceptance of unlawful settlement terms or engaging in premature litigation discovery, the CID must be quashed.¹⁸ For all of the reasons described above, the evidence is overwhelming that the CID was indeed issued for one or the other of those two purposes. The “facts” presented

¹⁸ The law is clear that government agencies may not abuse the judicial process by seeking and obtaining issuance of a CID for “illicit purposes.” *SEC v. Wheeling-Pittsburgh Steel Corp.*, 648 F.2d 118, 126 (3d Cir. 1981). To the extent Staff’s purpose in seeking the CID was to coerce WHR’s acceptance of Staff’s unlawful settlement terms, the illicitness of Staff’s purpose is self-evident. But Staff’s purpose in seeking the CID was just as illicit to the extent Staff hoped to use the CID to obtain discovery to be used by Staff in litigating against Wyndham once the Proposed Complaint was filed, because discovery of that sort is supposed to be sought and obtained by Staff not in the guise of completing an already-completed investigation, but rather under and subject to the Commission’s rules for adjudicative proceedings, as authorized by an Administrative Law Judge.

by the Letter Ruling in ostensible rebuttal of that evidence are not facts at all. The full Commission must therefore quash the CID.

E. Because Staff Has No Authority to Investigate the Information Security Practices at WHR's Affiliates and Service Providers, the CID Is Invalid Insofar as It Seeks Information and Documents Relative to Those Matters

As noted above in Part I.C, there is nothing in the Access Letter, the January 2008 Resolution, the CID, or the prior dealings of the parties that would permit a conclusion that the authorized scope of the WHR Investigation includes the information security practices at any WHR affiliate or service provider in regard to consumer information that they themselves collect. Moreover, Staff has refused to produce the internal documentation that would definitively establish whether Staff was ever authorized to expand the WHR Investigation in this fashion, and the Letter Ruling never addresses the issue. Accordingly, even were the Commission to uphold the Letter Ruling's conclusion that the CID is valid as applied to information security practices at WHR (which, for the reasons stated above, it should not), the CID must be quashed insofar as it purports to request documents and information relating to information security practices at any entity other than WHR or the Wyndham-branded hotels in regard to consumer information that such entity itself collects.

II. WYNDHAM HAS CLEARLY DEMONSTRATED THAT THE CID IS OVERLY BROAD, UNDULY BURDENSOME, AND INDEFINITE

The Letter Ruling's dismissal of Wyndham's arguments that the CID is overly broad, unduly burdensome, and indefinite relies upon misunderstandings regarding the law, the facts of the negotiations between Wyndham and Staff, and the facts related to the burden of responding to the CID. First, because Staff has not offered any justification whatsoever for believing that the security practices at WHR's affiliates are "reasonably relevant"¹⁹ to the investigation of security practices at WHR, Wyndham, by explaining why they are not, has met its burden of proving that the CID is overly broad. *See* Part II.A below. Second, Wyndham has provided sufficient evidence to show that the CID is overly burdensome, and neither Staff nor the Letter Ruling has questioned the accuracy of that evidence. *See* Part II.B below. Third, the Letter Ruling did not rebut Wyndham's claim that many of the requests contained in the CID are indefinite. *See* Part II.C below. For

¹⁹ *U.S. v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (Agency subpoenas or CIDs should not be enforced if they demand information that is: (a) not "within the authority of the agency," (b) "too indefinite," or (c) not "reasonably relevant" to the inquiry); *see also SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1025 (D.C. Cir. 1978) (noting that the subpoena request must "not [be] so overbroad as to reach into areas [that] are irrelevant or immaterial" and that specifications must not exceed the purpose of the relevant inquiry) (internal quotation marks and citations omitted).

each and all of these reasons, then, the CID must be quashed—whether or not it was validly issued (which it was not).

A. Wyndham Has Repeatedly Demonstrated That the Security Practices at WHR’s Affiliates in Regard to Customer Information They Themselves Collect Are Not Relevant to the WHR Investigation

The Petition identifies a number of ways in which the CID seeks information that is not reasonably related to any potential claim that Section 5 was violated with respect to the security surrounding data collected by the Wyndham-branded hotels from their customers. The Letter Ruling contested Wyndham’s irrelevance claim only as to one such category—documents related to the information security practices at Wyndham’s affiliates in regard to customer information that they themselves collect—on the illogical notion that because certain employees of these affiliates played a role in information security at WHR, the FTC is entitled to seek information regarding the information security practices and procedures at these affiliates in regard to customer information that they themselves collect—even though such practices and procedures by definition in no way relate to information security at WHR. The Letter Ruling should be overturned in this respect. First, the FTC does not have statutory authority to use compulsory process to seek discovery when it cannot articulate a reason to believe that the discovery sought would be reasonably related to a potential violation of the FTCA. *See* Part A.1 below. Second, Wyndham has met its burden of proving that the discovery sought by the CID is in numerous respects not reasonably related to any potential FTCA violation that Staff has under investigation. *See* Part A.2 below.

1. The FTC Does Not Have Authority to Use Compulsory Processes to Engage in a Fishing Expedition

In passing the Federal Trade Commission Improvements Act of 1980, Congress intended to create a statutory framework that would prevent the type of open-ended, cumbersome and expensive “fishing expeditions” in which the Commission had been engaged prior to the enactment of the 1980 amendments.²⁰ *See* Petition, Exhibit A hereto, at 18-26. The reforms passed in the Federal Trade Commission Improvements Act of 1980 thus not only “require[d] that the Commission state the nature of the conduct constituting the alleged violation under investigation and the applicable provision of law,” but also “include[d] appropriate safeguards to protect the legitimate rights and interests of every person subjected to investigation.” S. Rep. 96-500, at 1107. The 1980 Senate Report is

²⁰ See Senator Heflin’s arguments in favor of the CID statute, in which he observed that the difference between the information that the staff sought in its subpoenas and the information it really needed could *literally* amount to the difference between a truckload of documents and a large manila envelope full of documents. 126 Cong. Rec. 2395 (1980).

accordingly replete with references to the purpose of the CID provision and the protections therein: curtailing FTC investigations of impermissibly broad scope, so-called “fishing expeditions.”²¹

The Letter Ruling thus ignores congressional intent in stating that “[c]ourts . . . place the burden on Petitioners to show that the Commission’s determination is ‘obviously wrong’ and that the information is irrelevant.” Letter Ruling, Exhibit C hereto, at 7. Contrary to this statement, Staff’s burden before the Commission is to “describe with specificity the information needed, the reasons why the information is relevant to the inquiry, and the cost and burden production will impose on target companies” and to “explain why the information is not available through alternative (voluntary) means.” S. Rep. 96-500 at 1127; *see also* Petition, Exhibit A hereto, at 21. Here, as detailed below, the Letter Ruling offers no basis for believing that any such showing was or could have been made before the Commission in regard to numerous aspects of the CID. The CID thus fails to comport with Congress’s intent to curb “fishing expeditions” by Staff in the course of Commission investigations.

2. The Letter Ruling Does Not Rebut Wyndham’s Arguments that Numerous Categories of Documents and Information Sought by the CID Are Irrelevant to the WHR Investigation

The Letter Ruling describes the WHR Investigation as “focuse[d] on a series of breaches of WHR’s data security processes.”²² However, Wyndham demonstrated in the Petition the numerous ways in which the CID seeks documents and other information that cannot possibly be relevant to a claim that WHR or any other entity violated Section 5 in relation to data security practices and procedures *at WHR*. Petition, Exhibit A hereto, at 33-36. With respect to the majority of categories identified by Wyndham as being overbroad in this fashion, neither Staff nor the Letter Ruling have articulated any counterarguments as to how documents and information falling in the category in question are reasonably related to Staff’s investigation of the adequacy of WHR’s information

²¹ *See* S. Rep. 96-500, at 1105 (“The FTC’s broad investigatory powers have been retained but modified to prevent fishing expeditions undertaken merely to satisfy its ‘official curiosity.’”); *id.* at 1107 (noting that the CID provision “[was] designed to curtail the issuance by the Commission of overly broad subp[on]enas for the purpose of investigating unfair or deceptive acts and practices as defined in Section 5 of the FTC Act.”); *id.* at 1124 (amendments are a response to “testimony on the issuance of overly broad industrywide subp[on]enas by the Commission for the purpose of investigating unfair or deceptive acts and practices as defined in Section 5 of the Act.”).

²² Letter Ruling, Exhibit C hereto, at 7.

security practices.²³ As to those categories, then, the CID certainly must be quashed; indeed, there is no basis in the record for the Commission to do otherwise. Further, with respect to the one overbroad category that *is* discussed in the Letter Ruling, there is no logic whatsoever to the Letter Ruling's statement that because "WHR's data security processes . . . are managed by other Wyndham entities," Staff is entitled to look at "information security systems developed by Petitioners and their affiliates" in regard to customer information that they themselves collect.²⁴ The information security systems developed by WWC, WHG, and WHM with respect to the data *they* collect from *their* customers are both physically and logically distinct from the whatever information security systems one or more of these entities may have developed for WHR.²⁵ Further, Wyndham's citations to the multiple places where Staff has advanced this illogical argument plainly does not, as the Letter Ruling feebly contends, constitute an "admission" by Wyndham as to the correctness of that argument.²⁶ Because Wyndham has presented well-reasoned arguments as to how the information sought by the CID is in numerous respects not relevant to the investigation, and the FTC has not offered any justifications to the contrary, Wyndham has met its burden of showing that the CID is overly broad with respect to each of the categories so characterized by the Petition.

²³ These categories include documents generated during, or information relative to, the period between May of 2010 and December of 2011; information and documents regarding any and all "Service Providers" who were allowed access to personal information relating to WHR's customers; "personal information" other than the type that was allegedly placed at risk of compromise during the Intrusions; the dates on which the Wyndham-franchised and managed hotels entered into franchise and management agreements with WHR; the identity of the members of the Board of Directors of WHR and each of its affiliates and the length of time he or she has served in such a role; and the process that WHR's quality assurance program uses to assess the Wyndham-branded hotels' compliance with their contractual obligations. See Petition, Exhibit A hereto, at 33-34.

²⁴ Letter Ruling, Exhibit C hereto, at 7.

²⁵ WHG's responsibility for managing WHR's information security systems ended in July of 2009, when the information security function for WHR was subsumed within Wyndham's information security function. Therefore, there can be no argument that any documents relevant to WHG created after July 2009 are relevant to the WHR Investigation. Moreover, WHM does not play a role in the WHR information security function.

²⁶ The Letter Ruling argues that "as Petitioners admit, Commission staff provided an explanation of the relevance of these requests." Letter Ruling, Exhibit C hereto, at 7. This "admission," however, was merely a restatement of Staff's prior argument for the purpose of pointing out its flaws. The citation in support of this alleged admission points to a page in the Petition where Wyndham notes that Staff's "sole argument in defense of the requests" is that "WHR's affiliates are relevant because information security services were provided to WHR by WHG and later by WWC, and to the managed Wyndham-branded hotels by WHM" but that Staff has "fail[ed] to state any reason why information or documents related to the separate information security programs of these entities themselves, and unrelated to information security at WHR or the Wyndham-branded hotels, are relevant to the WHR Investigation." Petition, Exhibit A hereto, at 33. The FTC should not be considered to have rebutted Wyndham's argument merely because it reasserted a prior argument that Wyndham has proven to be flawed.

B. Wyndham Has Proven that Responding to the CID Would Cause it to Incur Significant Burden

Even if Staff could justify all the requests contained in the CID as being reasonably related to the WHR Investigation (which it cannot), the Letter Ruling still must be overturned, because it fails to adequately consider the evidence presented by Wyndham that the CID is overly burdensome. First, Wyndham has provided evidence sufficient to show that the CID imposes on it a burden that is significant, even when viewed in the abstract. *See* Part B.1 below. Second, Wyndham has shown that the burden of the CID is absurd when measured against the indisputable fact that no consumer injury resulted from any violation of Section 5 that may have occurred. *See* Part B.2 below. Third, the Letter Ruling underestimates the burden of responding to the “documents sufficient to describe” requests. *See* Part B.3 below. Fourth, imposing on Wyndham the significant and absurd burden inherent in the CID has no realistic prospect of generating information regarding any potential Section 5 violation. *See* Part B.4 below. Fifth, the Letter Ruling mischaracterizes the meet and confer negotiations between Wyndham and Staff and overlooks the fact that Wyndham provided Staff with a proposal for modifying the CID that was both specific and reasonable. *See* Part B.5 below. Finally, the Letter Ruling’s suggestion that Wyndham provide documents in lieu of interrogatories does not reduce Wyndham’s burden in a significant manner, so long as Wyndham still has 127 requests to which it must respond. *See* Part B.6 below.

1. Wyndham Has Provided Sufficient Evidence to Show That the Burden that Would Be Imposed on It by the Effort to Comply with the CID Is Significant

Wyndham provided three key pieces of evidence to support its claim that the CID is unduly burdensome: (1) a particularized explanation in the Petition itself as to why the CID’s requests are difficult to respond to, *see* Petition, Exhibit A hereto, at 36-39; (2) the sworn Declaration of Korin Neff, Esq. (the “Neff Declaration”), in-house counsel for Wyndham, which described the financial and time costs voluntarily incurred by Wyndham in responding to the Access Letter and the anticipated costs of responding to the CID, *see* Neff Declaration, Exhibit B.4 hereto; (3) a set of formal objections to the CID, which noted for each request how the burden compared to the likelihood that Staff would ascertain admissible evidence from the response to said request, *see* Exhibit B.16 hereto. Neither Staff nor the Letter Ruling has suggested that the sworn statements provided in the Neff Declaration are inaccurate. Wyndham has, therefore, sufficiently shown that a burden

exists that merits, at minimum, substantially narrowing the CID, if not quashing it entirely.²⁷

Contrary to the Letter Ruling's assertion, Wyndham's estimate of the enormous burden that compliance with the CID would impose is both specific and detailed. The Neff Declaration provided information regarding the length of time it would take Wyndham to investigate the questions posed by the FTC and prepare responses, to review ESI for documents responsive to the FTC's requests, the costs of both these endeavors, including the elements that factor into the significant costs of the ESI review. *See* Neff Declaration, Exhibit B.4 hereto, at ¶¶ 9-12.²⁸ The type of detail provided by Wyndham regarding burden is the same type of detail provided by petitioners in similar cases where the FTC or district courts have found that petitioners sufficiently demonstrated that compliance with a CID or subpoena was overly burdensome.²⁹ Wyndham disputes the claim that the specific cost incurred in, for example, the processing of documents by an outside vendor stage as compared to the review of documents for responsiveness or privilege stage has any relevance to the question of whether a significant burden exists, since whether a burden

²⁷ *See Phoenix Bd. of Realtors, Inc. v. Dep't of Justice*, 521 F. Supp. 828, 832 (D. Ariz. 1981) (the government should negotiate to narrow scope of a CID when compliance may be overly burdensome).

²⁸ Indeed, Paragraph 9 appears to provide the very itemization that the Commission states on page 8 that the Petition lacked.

²⁹ *See Genuine Parts Co. v. FTC*, 313 F. Supp. 855, 857-58 (N.D. Ga. 1970) *aff'd* 445 F.2d 1382 (5th Cir. 1971) (limiting a FTC Order to File a Special Report where the court found many of the requests overly broad in that they covered too expansive a period of time, asked for specific information concerning numerous individual customers as opposed to numbers in the aggregate, and defined entities "affiliated in any way" far too broadly); *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F. Supp. 11, 12-14 (S.D.N.Y. 1994) (quashing the entirety of a grand jury subpoena because it unnecessarily sought irrelevant information including legions of electronic storage devices without any specificity as to what type of information was specifically sought from the storage devices); *CFTC v. McGraw Hill Cos.*, 390 F. Supp. 2d 27, 35-36 (D.D.C. 2005) (limiting the scope of a subpoena by the CFTC even though the information sought went "to the heart of the . . . investigation" because it was overly burdensome and arguably requested "all data from any source").

exists depends inherently on the cost of all the steps that in aggregate would be necessary to comply with the CID.³⁰

Moreover, contrary to the Letter Ruling's unsubstantiated claim, the estimate of burden provided in the Petition and the Neff Declaration *did* take into account Instruction K as well as the use of technology and contract attorneys where appropriate to optimize review efficiency. There is no support in any FTC rule, rule of civil procedure, or federal court case for the proposition that in order to establish burden, a party is *required* to provide the line-by-line details of its (likely privileged and proprietary) evaluation of how "the availability of e-discovery technology, such as advanced analytical tools and predictive coding," Letter Ruling Exhibit C hereto, at 8—or in general, to provide information about the workflow it intends to use to collect, search, and review documents or justification as to why it structured its workflow in a particular way.³¹ Wyndham has informed Staff on several occasions that in responding to the Access Letter WHR employed techniques such as hiring of an e-discovery vendor, search term filtering, and global de-duplication,³² and the cost estimate for future production accounts for the fact

³⁰ The Letter Ruling's failure to credit Wyndham's showing of burden may stem from a math error that the Letter Ruling made in Note 39. The total cost to produce the first two custodians in response to the requests contained in the Access Letter was \$2.8 million, or \$1.4 million per custodian. Neff Declaration, Exhibit B.4 hereto, at ¶8. Because Wyndham reviewed the ESI of the most relevant custodians in the prior round of review, it is estimated that as to additional custodians, search terms will hit on slightly fewer—albeit still a significant amount—of documents. Additionally, global de-duplication technology will result in the reduction of the data set for additional custodians, to the extent they communicated with the custodians already reviewed. Due to these factors, and knowledge gained by Wyndham regarding optimal workflow in the prior round of review, Wyndham estimates that the cost to produce three additional custodians would be \$1 million, or \$333,333 per custodian. Neff Declaration, Exhibit B.4 hereto, at ¶11. While, as described below, Wyndham denies that it produced documents that were not responsive to the FTC's prior requests or not contained in family containing such documents, the hours and therefore cost to load and review documents that are hit by search terms are the same regardless of whether those are ultimately coded responsive.

³¹ See *I Med Pharma Inc., v. Biomatrix, Inc.*, 2011 WL 6140658, *5 (D.N.J. Dec. 9, 2011) (discussing a showing of burden through the number of documents that need to be reviewed, the costs associated with reviewing the documents, and the time it would take to review those documents); *U.S. ex rel. McBride v. Haliburton Co.*, 272 F.R.D. 235, 240-41. (D.D.C. 2011) (discussing a showing of burden in the extent of prior productions, the lack of a specific rationale on behalf of the requestor for further productions, and the non-attorney costs associated with retrieving and preparing documents).

³² These methodologies are recognized as best practices in the conduct of electronic discovery, whereas, as described in note 33 *infra*, use of content-based advanced analytics have yet to be accepted by the legal community. See The Sedona Conference Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery, 8 Sedona Conf. J. 189, 200 (2007) ("The ability to perform keyword searches against large quantities of evidence has represented a significant advance in using automated technologies, as increasingly recognized by the courts."); District Court of Delaware, Electronic Discovery Default Standard, *available at* <http://www.ded.uscourts.gov/sites/default/files/Chambers/SLR/Misc/EDiscov.pdf>, (expressly endorsing use of search terms but making no mention of predictive coding).

that Wyndham intends to continue using technology as appropriate to the nature of the documents to be collected, searched, and reviewed in this matter.³³ See Sedona Conference, *The Sedona Principles (2nd Ed.): Addressing Document Production*, Principle No. 6 (“Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.”).

Further, the Letter Ruling’s contention that electronic evidence is cheaper to produce and that the production called for by the CID thus can be easily accomplished through technology is incorrect. While it is true that between a number of pages in electronic format and a number of pages in paper format,³⁴ the electronic pages are likely less costly to review because of the capability to search the documents using key words, it is equally true that increased reliance on technology has caused the amount of data that exists to be collected, searched, and reviewed in a discovery process to grow exponentially in recent years. See *I Med Pharma Inc.*, 2011 WL 6140658, *5 (D. N.J. Dec. 9, 2011) (“Even if junior attorneys are engaged, heavily discounted rates are negotiated, and all parties work diligently and efficiently, even a cursory review of that many documents will consume large amounts of attorney time and cost millions of dollars”).³⁵

³³ The Letter Ruling’s implication that predictive coding is an easy solution to culling large amounts of data drastically oversimplifies the issue. Predictive coding, or “content-based advanced analytics” is a complex, relatively new, and largely untested methodology for reviewing documents. Few studies exist regarding its effectiveness, and only one magistrate judge in the entire country has ever endorsed its use (in a decision that has been objected to). A recent dispute regarding the use of the technology in a case in the Northern District of Illinois required two full days of expert testimony at an evidentiary hearing on the matter, and that dispute remains unresolved. See *Kleen Products, LLC v. Packaging Corp. of America*, case no. 1:10-cv-05711 (N.D.Ill.).

³⁴ This, in fact, was the point that Judge Shira Scheindlin was expressing in the *Zubulake* case cited by the Commission. See Letter Ruling, Exhibit C hereto, at 8 n.38. Nowhere in the *Zubulake* opinion does Judge Scheindlin state that because electronic evidence is searchable, there is no or minimal burden to producing it. See *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003); see also *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities LLC et al.*, 685 F. Supp.2d 456, 461 (S.D.N.Y. 2010) (Scheindlin, J.) (“In an era where vast amounts of electronic information is available for review, discovery in certain cases has become increasingly complex and expensive.”).

³⁵ See also, e.g., *B&B Hardware, Inc. v. Fastenal Co.*, 2011 U.S. Dist. LEXIS 150543, at *25 n.10 (E.D. Ark. Dec. 16, 2011) (“Much e-discovery is highly technical in nature and not the type of services that attorneys or paralegals are able to provide without assistance from IT specialists, whether from in-house staff or outside vendors”); Shelley Podolny, *The Digital Pileup*, N.Y. TIMES, Mar. 12, 2011, http://www.nytimes.com/2011/03/13/opinion/13podolny.html?_r=2&scp=5&sq=e-discovery&st=nyt (“In addition, large corporations face eye-popping litigation costs when they search for information that may be evidence in a lawsuit —so called e-discovery—that can add up to millions of dollars a year”); Steven C. Bennett, *Are E-Discovery Costs Recoverable by a Prevailing Party?*, 20 Alb. L.J. Sci. & Tech. 537, 538 (2010) (“The costs of electronic discovery can be crushing”).

Instruction K does not work to reduce the burden that would be imposed on Wyndham, as it will require Wyndham to re-review over 1 million pages of documents that it has already produced as well as the documents of several additional custodians. Moreover, to code the documents by request as the Letter Ruling seems to interpret Instruction K to require, Wyndham would have to compare each and every document against each of the 127 interrogatories and document requests contained in the CID. Such a review would be incredibly time-consuming and pointless in light of the fact that, presumably, the FTC has already reviewed these documents and determined which are relevant to the particular issues it claims in the CID to be interested in investigating.

2. The Burden That Would Be Imposed by the CID Is Disproportionate to the Issues at Stake in This Matter

The Letter Ruling errs in stating that the burden imposed by the CID should be “evaluated in relation to the size and complexity of a recipient’s business operations.” Letter Ruling, Exhibit C hereto, at 10.³⁶ By reason of this error, the Letter Ruling mischaracterizes or ignores Wyndham’s argument in the Petition that the burden imposed by the CID dwarfs what is at stake in the investigation since no consumer injury occurred. Petition, Exhibit A hereto, at 38. Under proper legal analysis, the burden of the CID should not be evaluated solely against Wyndham’s gross revenue as the Letter Ruling held, but rather against “what is at stake in the litigation.” *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 358 (D. Md. 2008). Thus, the touchstone is whether the “burden of discovery outweighs its utility.” *U.S. ex rel. McBride v. Haliburton Co.*, 272 F.R.D. 235, 240-41. (D.D.C. 2011). In order to evaluate whether the burden outweighs the utility from production, courts analyze “(1) the needs of the case; (2) the amount in controversy; (3) the parties’ resources; (4) the importance of the issues at stake in the action; and (5) the importance of discovery in resolving the issues. *Id.* (citing Fed.R.Civ.P. 26(b)(2)(C)(iii)). The Letter Ruling disregards the four other considerations in making this determination and instead focuses exclusively on Wyndham’s resources. Letter Ruling, Exhibit C hereto, at 10. Not only does the Letter Ruling ignore the majority of the factors to determine the

³⁶ The Letter Ruling relies on *FTC v. Texaco, Inc.*, 555 F.2d 862 (D.C. Cir. 1977) for the proposition that “the burden posed by this cost [i.e. the cost of complying with the CID] is evaluated in relation to the size and complexity of a recipient’s business operations,” and this the burden is acceptable so long as it “will [not] seriously disrupt [Wyndham’s] business operations.” Letter Ruling, Exhibit C hereto, at 10. However, *Texaco* provides an inappropriate standard for evaluating the burden of complying with a CID because the 1980 amendments to the FTC Act targeted *precisely* the kind of information demands that the FTC was then leveling at companies like Texaco. In explaining the need for the CID provision, Senator Heflin specifically noted that “[o]ne company (Texaco) reported that it had used 700 people working 7,000 man-hours at a cost of \$200,000 just to evaluate the burden that the proposed subp[ro]na would impose, if it were enforced. [Texaco and other] companies’ estimates of that potential burden reveal staggering figures.” 126 Cong. Rec. 2395 (1980).

burden imposed by the CID, but it also creates a system where a large company would be subject to unlimited discovery by the FTC on mere suspicion of an FTC Act violation merely because it has significant annual revenues. The large company would be forced to comply with every discovery request no matter the minimal importance of the action or invasiveness to the company. The Letter Ruling ignored or discounted that “[t]he goal is to attempt to quantify a workable ‘discovery budget’ that is proportional to what is at issue in the case.” *Mancia*, 235 F.R.D at 364. The concept of proportionality is especially heightened in the e-discovery arena.³⁷

The proportionality analysis missed by the Letter Ruling is especially significant because no consumer injury occurred here, and the Letter Ruling’s suggestion that consumer injury may have resulted from the intruder’s access to payment card information is simply wrong. Card brand rules prevent cardholders from suffering any financial injury if a third party gains access to their card information. Tellingly, Staff has not included an unfairness claim in the Proposed Complaint, presumably because Staff (though evidently not Commissioner Brill) realizes that such a claim would require an impossible-to-make showing of consumer injury. Similarly, Staff has not pointed to how any of the additional documents sought by the CID, coming as they would on top of the more than one million documents already produced, can be expected to indicate any Section 5 culpability on the part of WHR that Staff has not already (in its view) found to exist. If Wyndham’s compliance with the CID were truly necessary in order for Staff to be able to complete the WHR Investigation, Staff should be able to easily identify why the CID’s additional document requests and interrogatories would “make the existence of some crucial fact more likely than not.” *U.S. ex rel. McBride*, 272 F.R.D. at 241 (holding that the defendant had already spent a “king’s ransom” (over \$650,000 responding to discovery requests) and that “[w]ithout any showing of the significance of the non-produced emails...the search relator demands cannot possibly be justified when one balances its cost against its utility”). In sum, since no consumer injury occurred, the issues at stake are minor, and Wyndham has already provided extensive amounts of information and documents to Staff, the CID fails the proportionality analysis and should be quashed or, at a minimum, severely limited.

³⁷ See Institute for the Advancement of the American Legal System, Final Report on the Joint Project of the American College of Trial Lawyers Task Force on Discovery and the Institute for the Advancement of the American Legal System, at 14 (2009), available at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCQQFjAA&url=http%3A%2F%2Fwww.actl.com%2FAM%2FTemplate.cfm%3FSection%3DHome%26template%3D%2FCM%2FContentDisplay.cfm%26ContentID%3D4008&ei=zQmMT6fmO9HKrAeA2YW9Cw&usg=AFQjCNH-R_HsvguXkWtz1WHoZTeHIDg16A (noting that the respondents “told us that electronic discovery is a nightmare and a morass. These Principles require early judicial involvement so that the burden of electronic discovery is limited by principles of proportionality.”).

3. The “Documents Sufficient to Describe” Requests Impose Significant Burden Because of Their Vague and Overly Broad Nature

The fact that certain of the CID’s requests are limited to seeking “documents sufficient to describe” a particular matter rather than “all documents” relating to a matter actually could impose a greater, not lesser, burden on Wyndham because it may force Wyndham to conduct two reviews—one to fully search electronic systems to determine which documents exist that could shed light on the subject of the request, and a second to determine which of those documents, taken together, fully and completely show the information demanded by the CID. This problem is made worse by the fact that the CID is overly broad in the respects described above, and because the language used in the requests is vague and indefinite. For example, Request No. 6(d) seeks documents sufficient to describe “the technical configurations of devices and programs [each Wyndham entity] 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.” CID, Exhibit B.1 hereto. This is an incredibly broad request because Information Security Program is defined to mean “policies, practices, and procedures to protect personal information,” and virtually every attempt to control access to a Wyndham entity network, machine, or location of stored data in some way relates to the protection of all data stored on that entity’s network, and because technical configurations (which is a vague term in itself) have changed numerous times during the time period. To respond to this request, each of the WWC, WHG, WHR, and WHM entities would first have to make a list of all hardware devices used to protect against unauthorized access, since the first defense against unauthorized access to personal information is preventing the intruder from entering the network generally. Next, each entity would have to determine what antivirus program, anti-malware programs, log monitoring programs, and other software defenses are installed on each and every user machine and server in the company. Then, Wyndham would have to conduct an extensive electronic review of files related to these machines and files belonging to Information Security/Informational Technology personnel for documents that relate to technical configurations of the hardware and programs. After having identified those documents, Wyndham would have to conduct a second review of those documents to pull out the ones that sufficiently describe the technical configuration and check those documents against the list of devices and programs identified to ensure that the documents describe each configuration that existed for all devices. The Letter Ruling can hardly argue that this is a simple task.

4. The Utility of Further Document Production is Minimal at Best

The Letter Ruling does not challenge the assertion by Wyndham in the Petition that it is nearly impossible, when one considers the elements of the FTC’s potential claims

against Wyndham, that Wyndham's response to any request contained in the CID will lead to the discovery of information that will allow the FTC to build a case against Wyndham. *See* Petition, Exhibit A hereto, at 38. The Proposed Complaint that Staff has provided to Wyndham contains a single deception-based Section 5 claim, yet only one of the 127 requests relates to statements made to customers (Document Request No. 15), and WHR already responded to an identical request in its response to the Access Letter. *See* Access Letter, Exhibit B.3 hereto, at Question 13. Staff also cannot expect to discover evidence to support its unfairness claim in a response to the remaining 126 requests because Staff has no way of demonstrating that the substantial consumer injury required to make such a claim occurred. *See* Petition, Exhibit A hereto, at 39.

The Letter Ruling argues that the fact that Wyndham has "already produced information does not establish . . . that staff has sufficient information," Letter Ruling, Exhibit C hereto, at 10, but does not point to a single discrete topic on which Wyndham has failed to provide sufficient information to satisfy Staff's investigatory objective. Further, if Wyndham's prior response failed to provide Staff with sufficient information to determine whether a violation of Section 5 had been committed, it is difficult to see how propounding the same exact requests again will result in the production of previously undiscovered relevant information. *See* Declaration of Douglas H. Meal, Exhibit B.2 hereto, at ¶¶ 10-11 and Exhibits B.2C and B.2D (noting that WHR has responded at least in part to 42 of the 89 interrogatories and 25 of the 38 document requests contained in the CID). The only new information that the FTC can hope to receive if Wyndham responds to these requests again relates to the information security practices and procedures practiced at entities other than WHR with respect to the data they collect from their customers, which is practically guaranteed to be useless because, as described above, these practices and procedures have nothing to do with the protection of WHR's customer data. To the extent that the other Wyndham entities have documents that relate to their role in managing information security at WHR, WHR has already produced those documents.

The fact that Staff believes that many of the documents produced in response to its prior requests are irrelevant further underscores the futility of further document production.³⁸ The Access Letter requested, among other things, that Wyndham:

³⁸ Because the FTC has not identified any specific documents that it believes were not relevant, Wyndham cannot comment specifically on why these documents were produced. *See* Letter Ruling, Exhibit C hereto, at 9 n.39. It should be noted, however, that the Access Letter required production of "complete copies of all documents and materials requested, even if you deem only a part of the document to be responsive", Access Letter, Exhibit B.3 hereto, at 2 (emphasis in original), it is possible that certain documents were produced that are not responsive on their face but may be members of responsive families. Documents such as software licenses, for example, may have been attached to emails that related to the use of the software program to bolster data security at WHR. Human resource records may have referred to the performance of individuals with respect to managing information security events. Magazine and newspaper articles may have reflected the level of knowledge and awareness that employees had regarding certain data security risks.

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: . . .
(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;

Access Letter, Exhibit B.3 hereto, Request 9. Because what constitutes a security procedure, practice, policy, or defense is so broad, and because the most relevant custodians were individuals whose daily job it is to consider, assess, and improve security procedures, practices, policies, or defenses, Wyndham informed Staff in the spring of 2010 that the request was likely to result in the production of numerous documents related to things like firewall settings and program configurations that would not actually shed light on the larger question of whether WHR employed reasonable security measures. Staff rejected WHR's suggestion that the scope of this request be narrowed, yet now complains that WHR produced too many non-relevant documents in response to this request. And though Staff feels that the prior response included significant amounts of non-relevant information, Staff has issued a document request in the CID that mirrors this request.³⁹

5. Wyndham's Efforts to Meet and Confer Regarding the CID Were Rebuffed by the FTC

The Letter Ruling mischaracterizes the history of negotiations between Staff and Wyndham prior to Wyndham's filing of its Petition. Wyndham participated in a telephone meet and confer on January 6, 2012 in which it presented to Staff its position that many of the requests of the CID lack relevance, impose an impermissible burden, and are indefinite. On January 8, 2012, counsel for Wyndham sent a letter to Staff documenting the specific proposal Wyndham had made during the January 6, 2012 call for narrowing of the CID in response to the stated objections. *See* January 8, 2012 Letter from Douglas H. Meal, Exhibit B.10 hereto, at 5-6. The "caps" offered by Wyndham in this proposal were not "arbitrary" but in fact reasonably related to the stakes in the potential litigation and the large amount of discovery conducted prior to the issuance of the CID. And Wyndham's proposed limits were significantly more generous than what the FTC would have been able to obtain under the Federal Rules of Civil Procedures or its own rules. *See* Petition, Exhibit A hereto, at 36. For example, Wyndham's suggestion that the ESI of three additional custodians be reviewed in an effort to locate documents responsive to the CID's "all documents" requests was not arbitrary at all, in light of the fact that the prior review of the two most relevant custodians' ESI did not yield a single document that Staff has identified as having been useful to the WHR Investigation and instead, as Staff

³⁹ CID, Exhibit B.1 hereto, Request 6 (Seeking information regarding the Information Security Program, defined as "policies, practices, and procedures to protect personal information," of each Wyndham entity).

acknowledges, yielded a significant number of documents that were wholly irrelevant to the investigation.⁴⁰ Staff thus agreed with Wyndham that “this is a reasonable suggestion.” See January 12, 2012 Letter from Kristin Krause Cohen to Douglas H. Meal, Exhibit B.11 hereto. Wyndham wrote to Staff on January 13, 2012 to express its desire to continue the meet and confer process, but noted that unless Staff was willing to extend the January 20, 2012 deadline for filing the Petition, such discussions would have to occur after the Petition’s filing, as Wyndham’s resources would be consumed by the Petition in the ensuing week. See January 13, 2012 Letter from Douglas H. Meal to Kristin Krause Cohen, Exhibit D hereto. Staff never responded to that communication and never attempted to resume the meet and confer process after January 20, 2012.

Wyndham remains open to discussions with Staff regarding narrowing the CID requests.

6. Responding to Interrogatories By Identifying Documents is Equally Burdensome Due to the Large Number of Interrogatories and Documents Implicated

The Letter Ruling’s offer to allow Wyndham to respond to the interrogatory requests by producing documents instead of a narrative response may ease the burden with respect to certain requests, assuming the definitions are narrowed as described by Wyndham in the Petition and objections, and Wyndham welcomes the opportunity to meet and confer with Staff as to which interrogatories would be appropriate for this change of instruction. However, because of the sheer number of interrogatories (89) and the breadth of these interrogatories, the reduction in Wyndham’s overall burden would be slight. The change in instruction would turn most of the interrogatories into documents sufficient to describe requests. As described in Point II.B.3 above, where such requests relate to broad topics for which business records showing the information is not maintained in the ordinary course of business, identifying which specific documents provide the information is more—not less—burdensome. For example, Interrogatory 12(f) requests Wyndham to identify, with respect to each Wyndham entity and the Wyndham branded-hotels “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.” (Emphasis added). Since a security practice could be as simple as changing a firewall setting or resetting a password, the scope of this request is incredibly broad, and Wyndham could never be sure that it has

⁴⁰ Though Staff has been in possession of organization charts showing individuals responsible for the information security function at WHR for over two years and has received over 1 million pages of documents which reveal which individuals were involved in key information security decisions, it has never suggested the name of any additional custodians whose documents it believes to be relevant to this investigation.

provided documents that show “all” security procedures, practices, policies, and defenses because minor changes or practices may not have been documented in readily accessible sources. Further, as described above, a review that requires document reviewers to code which of each 127 interrogatory and document requests each and every document is responsive to would be slow and burdensome to conduct.

For these six reasons, Wyndham reasserts that it has provided sufficient information to prove the burden that would be imposed on it by compliance with the CID and requests that the Commission overturn the Letter Ruling on this ground.

C. The Letter Ruling Fails to Rebut Wyndham’s Claim that the CID is Indefinite

The Letter Ruling does not discuss Wyndham’s argument, Petition, Exhibit A hereto, at 39-40, that the CID should be quashed because the requests are too indefinite. The Letter Ruling claims that this argument restates the objections made in arguments regarding irrelevance and burden. *See* Letter Ruling, Exhibit C hereto, at 11. In fact, while Wyndham agrees that the arguments are related, the claim that the CID’s requests are indefinite stems from distinct grounds. *See U.S. v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (citing indefiniteness as one of three bases for quashing CID); *see SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512, 514 (10th Cir. 1980) (confirming that “[t]o obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”). Even if Staff were to narrow the number of interrogatory and document requests, or revise definitions to narrow the requests to relevant targets, the vague wording of certain requests would still hamper a meaningful response. The Letter Ruling does not rebut the arguments advanced in the Petition with respect to indefiniteness.

CONCLUSION

For all of the foregoing reasons, as well as those set forth in the Petition to Quash and its accompanying exhibits, and the exhibits accompanying this Appeal, Wyndham respectfully requests that the Commission overturn the Letter Ruling and quash, or alternatively, limit the CID as described in the Petition.

Donald S. Clark

- 36 -

PUBLIC
April 20, 2012

Please do not hesitate to contact me if you should have any questions regarding this request for review by the full Commission.

Very truly yours,



Douglas H. Meal

Enclosures

cc: Seth Silber, Esq.

CERTIFICATE OF SERVICE

I hereby certify that, on April 20, 2012, I caused the original, twelve (12) copies, and a compact disc of Wyndham Worldwide Corporation and Wyndham Hotels & Resorts, LLC's Request for Full Commission Review of Letter Ruling Denying in Part Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation's Petition to Quash or, Alternatively, Limit Civil Investigative Demand, with attached exhibits, to be hand delivered to the Secretary of the Federal Trade Commission at the following address:

Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, D.C. 20580

A handwritten signature in black ink, appearing to read "David T. Cohen", written over a horizontal line.

David T. Cohen

PUBLIC

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

IN THE MATTER OF)
WYNDHAM HOTELS & RESORTS, LLC) **FILE NO: 1023142**
_____)

**Petition of
Wyndham Hotels & Resorts, LLC
and
Wyndham Worldwide Corporation to
Quash or, Alternatively, Limit
Civil Investigative Demand**

Submitted by:

**Seth C. Silber, Esq.
Wilson Sonsini Goodrich & Rosati**

**Douglas H. Meal, Esq.
Ropes & Gray LLP**

Dated: January 20, 2012

PUBLIC

TABLE OF CONTENTS

	Page
INTRODUCTION	1
BACKGROUND	3
ARGUMENT	14
I. THE CID IS INVALID.....	15
A. The CID is Not Predicated on a Proper Investigational Resolution	16
B. The CID Was Not Issued Based on the Required Showing of Need for Compulsory Process to Be Used in the WHR Investigation.....	20
C. The CID Does Not Inform WHR and WWC of the Purpose and Scope of the WHR Investigation or of the Nature of the Conduct Constituting Their Alleged Section 5 Violation or of How Section 5 Allegedly Applies to Their Conduct	23
D. The CID Was Issued for the Improper Purpose of Either Coercing WHR’s Acceptance of Unlawful Settlement Terms or Engaging in Premature Litigation Discovery (or Both).....	26
E. Because Staff Has No Authority to Investigate Employee Injuries or the Information Security Practices of WHR’s Affiliates and Service Providers, the CID Is Invalid Insofar As It Seeks Information and Documents Relative to Those Matters	28
1. Staff Has Not Been Authorized to Investigate Employee Injuries or the Information Security Practices of WHR’s Affiliates and Service Providers	29
2. The FTC In Any Event Has No Jurisdiction to Investigate Employee Injuries	31
II. THE CID MUST BE QUASHED BECAUSE IT IS OVERBROAD, UNDULY BURDENSOME, AND TOO INDEFINITE.....	32
A. The CID Is Pervasively Overbroad Because Request After Request Seeks Information Not Reasonably Related to the WHR Investigation	33
B. The CID Is Unduly Burdensome	36
C. The CID Is Too Indefinite in Numerous Respects.....	39
CONCLUSION.....	40

INTRODUCTION

Wyndham Hotels and Resorts, LLC (“WHR”) and its parent company, Wyndham Worldwide Corporation (“WWC” and, jointly with WHR, “Wyndham”), respectfully submit this Petition to Quash or, Alternatively, Limit the Civil Investigative Demand (“CID”) issued by the Federal Trade Commission (“FTC” or “Commission”) on December 8, 2011.¹

The sequence of events that culminated in Wyndham’s instant petition began nearly four years ago, when WHR became one of the thousands of American businesses, non-profits, and government agencies (the FBI and Department of Justice being the two latest examples) targeted by the scourge of criminal hackers bent on stealing cyber data. In WHR’s case, the criminals targeted payment card data being handled by a group of independently owned hotels operating under the “Wyndham” brand pursuant to a franchise or management franchise agreement with WHR or one of its affiliates. While the hackers may have succeeded in obtaining a limited amount of payment card data from some of the hotels, no personal information other than payment card data was compromised. Moreover, because card brand rules protect cardholders from suffering any financial injury when their card is compromised, no consumer suffered any injury as a result of this particular hack. Nonetheless, in 2010 the FTC decided to launch an investigation into whether WHR’s information security practices violated the federal consumer protection statute. WHR cooperated fully with that investigation over the next two years, without hearing a word from the FTC suggesting otherwise. However, notwithstanding WHR’s spotless record of full cooperation with the investigation, in December 2011 the Commission suddenly decided to seek to use compulsory process to further its investigation and, to that end, served Wyndham with the CID.

The CID suffers from the same flaws recently recognized by a federal district judge with respect to another FTC CID:

The court agrees with plaintiff that the CID appears on its face to be unconscionable, overburdensome and abusive. The CID is so broad that it indicates that no meaningful discretion was exercised by the FTC officials who prepared it. As plaintiff suggests, the CID appears to have the potential to cause plaintiff to suffer intolerable financial and manpower burdens and an inexcusable disruption of its normal business activities.

D.R. Horton, Inc. v. Jon Leibowitz, Chairman, No. 4:10-CV-547-A, 2010 WL 4630210, at *3 (N.D. Tex. Nov. 3, 2010). Indeed, for a number of reasons the FTC CID at issue here is significantly *more* problematic than the one that was excoriated in the *Horton* case. To begin with, here the CID was issued almost two years after the FTC initiated the investigation to which the CID relates. By that time WHR had already incurred out-of-pocket costs in excess of \$5 million in cooperating fully and voluntarily with the voluminous discovery requests that the staff of the FTC (“Staff”) had heaped on WHR in the course of the investigation. That cooperation

¹ The CID is attached at Exhibit 1. On December 19, 2011, Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, agreed to extend the time for filing this Petition to Quash to January 20, 2011. Accordingly, this Petition is timely filed.

included providing Staff with more than one million pages of documents in response to 29 separate document requests (including subparts) made by Staff; making five separate written submissions to Staff responding to 51 separate written questions (including subparts) that Staff had interposed; and making seven separate in-person presentations to Staff to provide additional information requested by Staff and to respond to additional questions raised by Staff.

Even more concerning, issuance of the CID occurred *after* the investigation had already reached a point where, according to Staff's own statements, the purpose of the investigation had already been accomplished. Specifically, the CID issued only *after* Staff told WHR that Staff believed its investigation had found reasonable ground to conclude that WHR had violated Section 5 of the Federal Trade Commission Act ("FTCA"); *after* Staff presented WHR with a proposed complaint setting forth the alleged Section 5 violation Staff believed it had uncovered; and *after* Staff demanded that WHR agree to a settlement of Staff's alleged Section 5 claim. In other words, by the time the CID issued, Staff had by its own admission already obtained everything it needed in order to move the matter beyond the investigatory phase.

Tellingly, the CID also issued *after*—indeed *just days after*—WHR submitted a white paper to the Director of the FTC's Bureau of Consumer Protection demonstrating the unlawfulness of the Staff settlement terms being objected to by WHR. Staff defended the timing of the CID by claiming that its investigation was for some reason not "complete," even though WHR had already responded fully to all Staff's voluminous, previously submitted discovery requests, and Staff had already concluded that corrective action should be taken by the FTC to address a supposed Section 5 violation by WHR. Thus, while ostensibly the CID is merely intended to enable Staff to obtain limited additional discovery that Staff thinks it still needs, even at this late juncture, to finish its longstanding investigation, WHR believes otherwise.

The CID itself proves this point. The CID does not merely target a few stray informational items that Staff may have somehow missed in its sixteen-month investigatory effort. Instead, as drafted, the CID would require WHR and WWC to respond to 89 further interrogatories, including sub-parts, and 38 further document requests (again including subparts). Moreover, almost every single discovery request in the CID has been drafted first to define the subject matter of the request as broadly as imaginable and then to demand a response containing a mind-numbing level of detail. Compliance with the CID would thus entail months of work and millions of dollars of expense.

Worse still, the CID is in large part duplicative of the discovery requests Staff previously made during the course of this investigation; takes no account whatever of the voluminous amount of information that WHR has already provided in response to those requests; and seeks to effectuate an eleventh-hour expansion of Staff's investigation beyond WHR's information security practices and into the information security practices of WHR's service providers and affiliates, even though to date Staff's investigation has revealed nothing whatever calling into question the information security practices of those other entities. Further, the CID is not based on a proper Commission investigational resolution; was not issued based on the required showing of need for invocation of compulsory process in an FTC investigation; fails to provide WHR and WWC with the statutorily specified notice of Staff's claim and legal theory; seeks information related to various issues that are beyond Staff's authority; and obviously was issued for an improper purpose—namely, to coerce WHR's acceptance of the unlawful settlement terms

being insisted on by Staff or, failing that, to obtain pre-litigation discovery from WHR in the guise of purporting to complete an investigation that, judged by any standard, should be considered to have been completed months ago.

Perhaps worst of all, the Staff investigation that is the subject of the CID has already established that the information security practices being investigated caused *no consumer injury* and any deficiency in those practices has already been *fully rectified*. Indeed, Staff's inability to prove consumer injury of the sort that normally is (or ought to be) the touchstone of an FTC enforcement action is so clear here that Staff does not even propose to assert an unfairness-based Section 5 claim. Instead, Staff's proposed complaint is limited to a deception-based Section 5 claim. But even that claim presents insignificant consumer protection concerns, for the claim is based solely on a privacy policy published on WHR's website that there is no reason to believe was ever even read, much less relied upon in making a purchasing decision, by any appreciable number of WHR customers (if, indeed, by any at all), and because the validity of Staff's deception claim depends entirely on Staff's tortured reading of just two sentences in that multi-paragraph policy—a reading that is elsewhere expressly negated by the policy itself. In other words, Staff is asking Wyndham to suffer the enormous additional discovery burden embodied in the CID in order to support a Staff investigation that, after nearly two years, has found, *at most*, a single, alleged Section 5 violation that indisputably was inadvertent if it happened at all (which it did not), and that in any event did not harm a single consumer.

In short, the CID is fundamentally flawed in essentially every imaginable respect and should be quashed in its entirety or, at the very least, significantly limited.

BACKGROUND²

WHR and the Wyndham-Branded Hotels

WHR's principal business is to provide a variety of services to a group of U.S.-based, independently owned hotels (the "Wyndham-branded hotels") that are licensed to use the "Wyndham" brand name. The Wyndham-branded hotels together constitute an upscale chain of hotels located in key business and vacation destinations. During the period in question, there were approximately ninety Wyndham-branded hotels worldwide, all of which were independently owned by third parties unaffiliated with WHR.³ At that time, most of the Wyndham-branded hotels (the "franchised Wyndham-branded hotels") used the Wyndham brand name pursuant to franchise agreements with WHR, but about fifteen of them (the "managed Wyndham-branded hotels") were operated under the Wyndham brand name pursuant to a management agreement with WHR's sister company, Wyndham Hotel Management, Inc. ("WHM"), under which WHM managed the hotel on behalf of the hotel's owner.

² The accuracy of the factual statements made in the "Background" section of this petition is attested to in the Declaration of Douglas H. Meal (Exhibit 2 hereto) ("Meal Declaration"), at ¶ 3.

³ WHR has a minority economic interest in the Rio Mar hotel, which is one of the managed Wyndham-branded hotels. Also, WHR currently owns the Bonnet Creek hotel, which was not part of the Wyndham-branded hotel chain during the period in question.

The Intrusions

On three separate occasions during the period between June 2008 and January 2010, WHR and certain of the Wyndham-branded hotels suffered criminal intrusions into their computer networks (the “Intrusions”). During the course of the Intrusions, certain customer payment card data being handled by the intruded-upon hotels was placed at risk of compromise. Significantly, however, other than payment card data, no personal information of any consumer was placed at risk during the Intrusions. As a result, because payment card issuers protect their cardholders against suffering any financial injury by reason of their payment card data being compromised, the Intrusions did not cause, and could not have caused, any financial injury to any consumer.

Also, while the intruder(s) did gain access to WHR’s network and the networks of certain of the Wyndham-branded hotels during the course of the Intrusions, at all times the information technology assets of WHR’s affiliated entities such as WHM were physically distinct and logically separate from WHR’s network and the networks of the Wyndham-branded hotels. Moreover, the forensic evidence shows no evidence of any of those affiliated entities being impacted by the Intrusions. Thus, there is no evidence that customer data located at any of WHR’s affiliated entities was ever at risk of compromise in the Intrusions or that any of those affiliated entities ever suffered from information security deficiencies.

Subsequent to the occurrence of the Intrusions, substantial information security enhancements were put in place at WHR. In January 2011, an assessment of WHR’s network security by an independent Qualified Security Assessor (“QSA”) culminated in the QSA’s issuance of a Report on Compliance that attested to the WHR network’s full compliance with the Payment Card Industry Data Security Standard (“PCI DSS”). As for the intruded-upon Wyndham-branded hotels, each of them⁴ executed a “Technology Addendum” to its franchise or management agreement pursuant to which WHR was given substantial direct responsibility for and over information security for the portion of the hotel’s network that had been attacked in the Intrusions.⁵ Pursuant to the Technology Addenda, substantial security enhancements were then also made to the intruded-upon Wyndham-branded hotels’ networks.

Staff’s Investigation

By means of an access letter dated April 8, 2010 (the “Access Letter”), a copy of which is attached hereto as Exhibit 3, the Commission advised WHR that Staff was conducting a non-public investigation into WHR’s compliance with federal laws governing information security (the “WHR Investigation”). According to the Access Letter, the WHR Investigation was prompted by the Intrusions. The Access Letter stated that the WHR Investigation sought to

⁴ Those Wyndham-branded hotels that were going to be leaving the system were not asked to execute the Technology Addendum and were not provided the services contemplated thereby. Also, several continuing Wyndham-branded hotels did not actually execute the Technology Addendum, but they all nonetheless did permit WHR to perform the services contemplated by the Technology Addendum.

⁵ In regard to the managed Wyndham-branded hotels, because the Technology Addendum was structured as an amendment to the management agreement WHM had entered into with the owner of the hotel, WHM executed the Technology Addendum rather than WHR, and then as permitted by the Technology Addendum WHM arranged for WHR to perform the Technology Addendum on WHM’s behalf.

determine whether WHR's information security practices complied with Section 5 of the Federal Trade Commission Act ("Section 5").

The WHR Investigation proceeded for the ensuing 16 months. Because the Intrusions affected the networks of WHR and certain of the Wyndham-branded hotels, the WHR Investigation focused on the adequacy of the information security measures that were in place at the time of the Intrusions to protect personal consumer information being handled by the WHR network and the hotels' networks. In that regard, while the WHR Investigation did reveal that the intruder(s) had gained access to the networks of both WHR and certain of the Wyndham-branded hotels during the course of the Intrusions, the WHR Investigation revealed that only payment card data had been placed at risk of theft during the Intrusions. Payment card issuers, pursuant to their contracts with their cardholders, fully protect their cardholders from suffering any financial injury by reason of their payment card data being stolen. Thus, the WHR Investigation found no evidence that any *consumer* had suffered any financial injury by reason of whatever access to personal consumer information had occurred during the Intrusions.

Because there is no evidence that the Intrusions extended beyond WHR's network and the networks of the intruded-upon Wyndham-branded hotels, the WHR Investigation did not address, or have any reason to address, whether at the time of the Intrusions adequate security measures were in place to protect whatever customer data was located at WHR's affiliates and WHR's service providers. Indeed, as noted above, the Access Letter itself expressly stated that *WHR* was the proposed respondent in the WHR Investigation, and that the subject matter of the WHR Investigation was limited to *WHR's* information security practices. *See* Exhibit 3 hereto, page 1. Moreover, WHR is not aware of the FTC's having ever taken action, subsequent to the delivery of the Access Letter, to authorize the WHR Investigation's being expanded to extend to the information security practices of any of WHR's affiliates and/or service providers, or to notify WHR or any of its affiliates of any such expansion.

WHR cooperated fully with the WHR Investigation. To begin with, WHR produced to Staff over one million pages of documents in response to the 29 separate document requests (including subparts) contained in the Access Letter and ensuing Staff communications. All but three of those requests targeted either certain specified documents or documents "sufficient to show" certain specified matters. Each such "targeted document request" accordingly required WHR to engage in a file-research project to try to locate the particular documents that would meet the request. These file-research projects were, in the aggregate, enormously labor intensive and time consuming. For example, more than five months of work were required just to complete WHR's effort to locate the documents called for by the targeted document requests included in the Access Letter. Upon completing that effort, WHR reported to Staff that, with the exception of just two requests as to which no documents could be located, WHR believed it had succeeded in locating documents that satisfied all the Access Letter's 29 targeted document requests. Similarly, WHR believes it succeeded in locating documents that met all the targeted document requests contained in Staff's ensuing communications. Significantly, Staff has never once suggested it disagrees with WHR's view as to the completeness of WHR's response to Staff's targeted document requests.

Staff's document requests also included three requests that sought "all documents" responsive to the matter in question. In substance, those three requests sought all documents

relative to the Intrusions and to WHR's and the Wyndham-branded hotels' information security at the time of the Intrusions. WHR proposed, without any objection by Staff, that its primary effort to locate documents responsive to the "all-document requests" would be to review the electronically stored information ("ESI") of the personnel who had the most direct responsibility for handling those matters and who, as a result, were most likely to have custody of documents relating to those matters. To that end, WHR reviewed the ESI of one individual who played a central role in WHR's information technology function during the period in question, and a second individual who played a central role in WHR's information security function during that period. All responsive, non-privileged documents located by means of that custodian-based ESI review (which amounted to more than one million pages in the aggregate) were in turn provided to Staff. Upon receiving that production, Staff did reserve the right to request at some later time that WHR expand its custodian-based ESI review to additional custodians. Staff never indicated, however, that it felt WHR's voluminous production in response to the all-document requests was somehow insufficient to meet Staff's investigatory objective in posing those requests.

In addition, WHR submitted to Staff five separate detailed written narratives responding to the 51 separate questions (including subparts) posed in the Access Letter and ensuing Staff communications. Owing to the number of and specificity called for by Staff's questions, preparation of WHR's narrative responses proved to be extremely burdensome, requiring extensive research and laborious drafting efforts. In the aggregate, including attachments, those responses total 72 pages, single spaced. WHR intended for each response to address fully and to provide all non-privileged information required by the particular Staff questions referenced by the response. Here, again, Staff has never suggested that any of WHR's responses failed to do that.

Further, the Chief Financial Officer and the head of Information Security for WHR, and/or WHR's inside and outside counsel, made seven separate in-person presentations to Staff in an effort to address various questions Staff had raised. Those presentations addressed a wide variety of Staff requests for additional information, ranging for example from further detail regarding the information security measures and policies that WHR had in place at the time of the breach to the technical details of the separation of WHR's network from the networks of WHR's affiliates to the structure and methodology of WHR's quality assurance program. Each such presentation was specifically requested by Staff, and each required substantial research into the matter being presented, extensive preparation on the part of the personnel making the presentation (usually including preparation of a supporting PowerPoint and/or document binder), and significant time expenditure associated with attending and traveling to and from the presentation itself. WHR sought for each presentation to fully address the matter on which Staff had requested the presentation and, when questions arose during the presentation, endeavored to answer those questions either in the course of the presentation itself or by means of a follow-up communication. Staff has never suggested that any of these presentations did not succeed in achieving, from Staff's perspective, the investigatory objective Staff had in requesting the presentation.

As can be well imagined, the burden that all these Staff requests placed on WHR was simply enormous. The above-described custodian-based ESI review by itself cost more than \$2.8 million. *See* Declaration of Korin Neff, January 20, 2012 (Exhibit 4 hereto) ("Neff Declaration"), at ¶8. Through July of 2011, WHR's total out-of-pocket costs for outside counsel

and other consultants retained to assist WHR in dealing with the WHR Investigation exceeded \$5 million. *Id.* Virtually all of these costs were expended in responding to the Staff discovery requests described above. And, of course, those costs give no account to the substantial amount of time expended by WHR's own personnel in doing the massive amount of research required to locate the documents and information sought by Staff's requests.

Staff's Proposed Complaint and Proposed Consent Order

During the course of the WHR Investigation, Staff advised WHR that Staff believed its investigation had adduced information sufficient to give the FTC reason to believe that WHR's information security practices were in violation of Section 5. On July 20, 2011, Staff provided WHR with a proposed complaint and a proposed consent order. Significantly, Staff's proposed complaint (the "Proposed Complaint," attached hereto as Exhibit 45) made no claim that WHR's information security practices were "unfair" under Section 5. Presumably, Staff recognized that, with payment card data having been the only personal information placed at risk of compromise in the Intrusions, Staff could not establish the substantial consumer injury necessary to sustain an *unfairness*-based Section 5 claim. Instead, the Proposed Complaint alleged only that WHR had committed a single *deception*-based violation of Section 5. Staff's theory, as set forth in the Proposed Complaint, was that two sentences contained in the privacy policy published on WHR's website since early 2008 (the "Privacy Policy") had expressly represented that reasonable security measures to protect customer information were in place at both WHR and the Wyndham-branded hotels. According to Staff's allegations, that representation was inaccurate because (as ostensibly shown by the occurrence of the Intrusions) neither WHR nor the Wyndham-branded hotels in fact had reasonable information security measures in place to protect customer information from criminal intrusion during the period in question.

The relief that Staff's proposed consent order (the most recent version of which ("Staff's Proposed Consent Order") is attached hereto as Exhibit 6) sought from WHR had three basic components:

1. a prohibition on WHR's making future misrepresentations of the sort alleged in the Proposed Complaint, as well as a variety of other future misrepresentations related to data privacy, confidentiality, security, and integrity (*see id.* at Part I);
2. a mandate that WHR (a) establish, implement, and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected by WHR from or about consumers and (b) arrange for an independent assessor to conduct biennial reviews designed to evaluate WHR's compliance with that program (collectively, the "Affirmative WHR Relief") (*see id.* at Parts II and IV.A - IV.D); and
3. a mandate that WHR (a) cause each Wyndham-branded hotel to establish, implement, and maintain its own comprehensive information security program, (b) assess, through WHR's Quality Assurance Program, each Wyndham-branded hotel's compliance with its program and take certain measures to address any instance of a Wyndham-branded hotel's non-compliance with such program, and (c) arrange for the independent assessor's reviews also to evaluate WHR's compliance with its monitoring and enforcement

responsibilities regarding the Wyndham-branded hotels' comprehensive information security programs (collectively, the "Affirmative Hotel Relief") (*see id.* at Parts III and IV.E).

The Proposed Complaint also alleges that WHM (the WHR affiliate that manages the managed Wyndham-branded hotels on behalf of the owners of those hotels), Wyndham Hotel Group ("WHG"), the parent company of WHR, and WWC, the parent company of WHG, are jointly liable for WHR's alleged deception-based violation of Section 5. Based on that allegation, Staff's Proposed Consent Order would impose substantial obligations (collectively, the "Affiliate Relief") on WHM, WHG, and WWC. As to WHM and WHG, Staff's Proposed Consent Order seeks much the same relief from them as it would obtain from WHR, by imposing on each entity the exact same prohibition regarding future misrepresentations and the exact same mandates regarding its own information security as it would impose on WHR. *See* Ex. 3, Parts I-II. As to WWC, Staff's Proposed Consent Order would impose on it the exact same prohibition regarding future misrepresentations that Staff's Proposed Consent Order would impose on WHR, and it would require WWC to guarantee WHR's, WHG's, and WHM's performance of their obligations under the order, but it would not impose on WWC any mandate regarding its own information security. *See id.* at Parts I, II & IX.

The Parties' Settlement Negotiations

WHR strongly believes that it did not violate Section 5 in connection with the Intrusions or otherwise. Accordingly, from the inception of this investigation WHR has viewed a settlement as unwarranted and has thought the appropriate resolution was for the WHR Investigation to be closed. WHR remains firmly of that view today.

Still, when Staff asked WHR whether WHR wanted to discuss settlement of Staff's Section 5 claim, WHR agreed to do so. To begin with, Staff said the settlement it had in mind would involve no monetary relief. And in regard to affirmative actions required of WHR under the consent order that would be part of the settlement, Staff said the predominant intent of the order it envisioned would be to require WHR to continue to provide the same information security that by that point WHR was already providing for its own network and for the networks of the Wyndham-branded hotels. WHR therefore understood the settlement concept to be offering WHR the possibility of a near-term, low-cost alternative to the years of expensive, time-consuming litigation that likely would be required to validate WHR's position that it had no Section 5 liability in connection with the Intrusions. As such, that concept merited consideration in WHR's view, notwithstanding WHR's belief that it did not violate Section 5. Accordingly, WHR agreed to work with Staff to see if this settlement concept could be turned into settlement documentation acceptable to both sides.

During the period from late July to mid-September of this year, Staff and WHR conducted substantial negotiations over Staff's proposed settlement terms. Those negotiations resulted in agreement in principle being reached on many important points. However, a number of points of disagreement remained, including three core WHR objections to Staff's Proposed Consent Order. Those three objections are the following:

- *first*, WHR objected to a settlement being founded on a theory that WHR committed a

deception-based violation of Section 5;

- ***second***, WHR objected to those portions of the Affirmative Hotel Relief that would involve WHR's assuming direct responsibility for the Wyndham-branded hotel's information security in certain respects—*contrary to the fundamental business model that underpins franchising*; and
- ***third***, WHR objected to the Affiliate Relief (other than the portion of the Affiliate Relief that would oblige WWC and/or WHG to cause WHR to perform WHR's obligations under the order).

What made these features of Staff's proposed settlement documentation objectionable was that they each imposed a substantial business burden and/or a substantial business risk on WHR and/or its affiliates that went well beyond merely requiring WHR to continue to provide the very same information security WHR was at that point already providing for its own network and the Wyndham-branded hotels' networks. Moreover, these three aspects of Staff's proposed settlement documentation had no legal basis (given the facts of this particular matter) and were wholly unnecessary to address the concerns that had prompted the WHR Investigation (given that those concerns were fully addressed by provisions of the settlement documentation WHR was prepared to accept). WHR accordingly communicated to Staff that WHR could not accept a settlement that included these three aspects. Staff responded by indicating that management of the FTC's Bureau of Consumer Protection ("BCP Management") was insistent that a settlement would have to include all three aspects of Staff's proposed settlement documentation to which WHR had objected. WHR thereupon requested a meeting with BCP Management.

On November 21, 2011, in anticipation of such a meeting, WHR submitted to BCP Management a detailed white paper that demonstrated, in regard to each of WHR's three core issues, how each aspect of Staff's Proposed Consent Order being objected to by WHR

- lacked any lawful basis under Section 5 given the particular facts of WHR's case;
- would impose on WHR substantial business burdens and/or expose WHR to breach of contract claims from the Wyndham-branded hotels, third-party liability claims, and/or other unacceptable substantial business risks; and
- was, in light of the portion of Staff's proposed consent order that WHR *did not* object to, wholly unnecessary to achieve Staff's goal of protecting WHR's customers against future circumstances of the sort that prompted the WHR Investigation.

WHR's white paper is attached hereto as Exhibit 7. Shortly after WHR's submission of this white paper, BCP Management agreed to the meeting WHR had requested. The meeting occurred on December 15, 2011. At the meeting, WHR summarized the grounds for its three core objections to Staff's proposed settlement documentation, as detailed in WHR's white paper. Neither during the meeting nor at any other time has any representative of the FTC provided WHR with any rebuttal to the white paper's arguments that the settlement provisions being objected to by WHR are both unlawful and unnecessary. Nonetheless, as reflected in Exhibit 3 hereto, Staff's next (and last) draft of Staff's proposed settlement documentation continued to include all three components objected to by WHR. And, in the meantime, Staff served WHR and WWC with the CID.

The CID

The CID did not come as a complete surprise to WHR. In October 2011, shortly after WHR's settlement negotiations with Staff reached an impasse and WHR asked to meet with BCP Management, Staff had orally advised WHR that Staff believed it needed certain additional information in order to complete its investigation and, to that end, intended to ask the FTC to issue a civil investigative demand to WHR. Thereafter, in late October, Staff had orally requested that WHR provide a "certification" as to the completeness of the information and documents WHR had provided to Staff in response to the Access Letter and Staff's ensuing discovery requests. Staff explained this request by stating that WHR's provision of such a certification would enable Staff to limit the anticipated civil investigative demand to requesting only documents and information that had not been covered by Staff's prior discovery requests and WHR's responses to those requests, and that were necessary for the completion of the WHR Investigation. Staff and WHR thereupon negotiated and agreed upon an acceptable form of the requested certification, and WHR submitted the executed certification (a copy of which is attached hereto as Exhibit 8) to Staff on December 1, 2011.

The length and breadth of the CID did come as a surprise to WHR, however, particularly in view of the certification that had just days earlier been requested by Staff and provided by WHR. According to Staff's prior statements, the CID would be limited to seeking only whatever additional documents and information Staff legitimately felt were needed for the completion of the WHR Investigation, bearing in mind the enormous volume of documents and information WHR had provided to Staff during the first 16 months of the investigation. WHR seriously questioned, of course, why Staff would need *any* further discovery to complete the WHR Investigation, given where the investigation currently stood.⁶ But even assuming the WHR Investigation were not entirely complete at this juncture, WHR felt it certainly must be nearly complete, given the enormous amount of documents and information already provided by WHR and the legal paucity of Staff's investigational findings based on its review of all that material. WHR accordingly anticipated that the CID at most would include a handful of additional questions and document requests, carefully drafted so as to avoid duplicating Staff's prior requests and so as to target precisely the particular pieces of additional information Staff was looking for, all to ensure that Wyndham would not incur significant burden in responding to those additional requests.

Unfortunately, the CID was not drafted in anything remotely resembling this fashion. To the contrary, it is a classic "kitchen-sink" discovery request that takes no account whatever of Staff's previous requests and WHR's previous responses to those requests, and makes no effort whatever to avoid unduly burdening Wyndham in responding to the CID. Including sub-parts,

⁶ After all, Staff had previously advised WHR that, based on Staff's investigation to date, Staff had already determined that the evidence created reason to believe that WHR's information security practices violated Section 5 and Staff accordingly was prepared to recommend corrective action to the Commission in the form of a consent agreement. Indeed, Staff had already provided WHR with the consent agreement it was prepared to recommend to the Commission and a proposed complaint alleging violations of Section 5 on the part of WHR and certain of its affiliates. In WHR's view, any investigation that has reached a point at which Staff has made such a determination and is ready to make such a recommendation is by definition "complete," because once an investigation reaches that point Staff by definition has no need for any further information in order to conclude the investigatory phase of the case (see Operating Manual §1.3.4.4) and proceed with the next phase of the case.

the CID includes no fewer than *eighty-nine* further interrogatories and *thirty-eight* further document requests. The sheer volume of the discovery requests contained in the CID is exacerbated by the fact that the vast majority of the CID's requests duplicate, in significant part, one or more of the discovery requests previously made by Staff during the course of the WHR Investigation. Moreover, those of the CID's requests (or portions thereof) that do not duplicate Staff's prior requests instead seek, for the most part, information or documents that have nothing whatever to do with the subject matter of the WHR Investigation, such as documents and information relative to the information security practices of WHR's affiliates and service providers. Finally, almost every single discovery request in the CID has been drafted first to define the subject matter of the request as broadly as imaginable and then to demand a response containing a mind-numbing level of detail.

A case in point, by way of example only, is Interrogatory 12. As drafted, Interrogatory 12 purports to require Wyndham to describe in detail each and every aspect of any and all information security measures that Wyndham had in place at any time during the last four years, including the date on which each and every such aspect was implemented, each and every assessment, test, evaluation, monitoring action, or change that was made of or to any such aspect during such period, and the date of every such assessment, test, monitoring action, or change. No account is given in this interrogatory to the voluminous amount of information that Staff has already requested and received in regard to WHR's information security during the period in question. No effort is made in this interrogatory to zero in on any particular aspect of WHR's information security that Staff might have concerns about based on its investigation to date. Moreover, to the extent Interrogatory 12 seeks information not only relative to WHR's information security, but also relative to the information security measures that were in place at WWC, WHG, and WHM during the period in question, this interrogatory utterly ignores the fact that there is no reason whatever for the FTC to believe that any of these entities suffered from any information security deficiencies during the period in question. Worst of all, no attention is paid in this interrogatory to the obvious fact that any company's information security measures are routinely being assessed, tested, evaluated, monitored, and changed not just daily but minute-by-minute, such that the net effect of this interrogatory as drafted is to ask that Wyndham undertake the mind-boggling effort to create for Staff, somehow, a comprehensive daily history of every detail of every aspect of every feature of Wyndham's information security over a four-year period.

Nearly all of the CID's interrogatories and document requests suffer from the defective triad of (i) duplicating discovery requests Staff has previously made and WHR has already responded to, (ii) seeking documents or information that have nothing whatever to do with the WHR Investigation, and (iii) being drafted without any attention having been given to the generality of the request and the level of detail demanded by the request. *See, e.g.*, Interrogatories 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, and 21, and Document Requests 2-7 and 9-17 (all of which in substantial part duplicate discovery requests Staff has previously made and WHR has already fully responded to); Interrogatories 5, 6, 7, 8, 12, 13, 14, 16, 17, 18, 19, 20, and 21, and Document Requests 3, 6, 7, 8, 9, 10, 12, 13, and 16 (all of which, by addressing the information security practices of Wyndham's service providers and/or affiliates, seek information relative to matters that have not been part of the WHR Investigation

up to this point⁷ and as to which Staff has no basis now to expand its investigation); and Interrogatories 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, and 21, and Document Requests 2-7 and 9-17 (all of which are drafted to cover an extremely broad subject matter and to demand a minute level of detail regarding that subject matter).

Because the CID's discovery requests were drafted in such an utterly defective fashion, compliance with the CID would impose a monumental burden on Wyndham. Specifically, based on the 16-month effort that WHR required in order to respond to the discovery requests Staff previously made of WHR in the course of the WHR Investigation, Wyndham estimates that it would need between one and two years to complete its response to the even more burdensome discovery requests contained in the CID, and even then the response would be incomplete in significant respects. Moreover, based on the costs WHR incurred in undertaking the effort WHR made to respond to Staff's previous discovery requests, WHR estimates that Wyndham would incur out-of-pocket costs of no less than \$3.75 million were it required to respond to the CID as drafted.

Wyndham's Unsuccessful Effort to Resolve Its Objections to the CID

As noted above, Wyndham considers the CID to be objectionable in virtually every respect imaginable. To begin with, for a number of reasons the CID is legally invalid: it is not based on a proper Commission investigational resolution; it was not issued based on the required showing of need for invocation of compulsory process in an FTC investigation; it fails to provide WHR and WWC with the statutorily specified notice of Staff's claim and legal theory; it seeks information related to various issues that Staff has no authority to investigate; and—perhaps worst of all—it obviously was issued for an improper purpose, namely, to coerce WHR's acceptance of the unlawful settlement terms being insisted on by Staff or, failing that, to obtain pre-litigation discovery from Wyndham in the guise of purporting to complete an investigation that, judged by any standard, should have been deemed completed months ago. Moreover, the CID is both grossly overbroad (in that almost all of its requests either duplicate requests Staff has previously made and WHR has previously responded to or address matters that are utterly irrelevant to the WHR Investigation) and unduly burdensome (in that most of its requests are drafted so as to define the subject matter of the request as broadly as imaginable and then to demand a mind-numbing level of detail regarding that subject matter, all without any regard being given to the enormous amount of information WHR has already provided to Staff during

⁷ During the meet-and-confer teleconference regarding the CID that took place between Staff and Wyndham, Staff took the position that the WHR Investigation had from its inception extended to WHR's affiliates and their information security practices. Staff was incorrect in advancing this position. The Access Letter was addressed solely to WHR and expressly stated in its very first sentence that Staff was conducting "a non-public investigation into Wyndham Hotels and Resorts, LLC's ('Wyndham') compliance with federal laws governing information security." The third sentence of the Access Letter then stated that "[w]e seek to determine whether *Wyndham's* information security practices comply with Section 5 of the Federal Trade Commission Act" (emphasis supplied). While the Access Letter later incoherently purported to redefine the term "Wyndham" to include Wyndham's affiliates and a number of other entities for purposes determining the scope of the Access Letter's discovery requests, that redefinition did not alter the Access Letter's earlier clear statement that the sole entity actually under investigation by Staff was WHR and the only information security practices being investigated were those of WHR. See Exhibit 3. Moreover, WHR is aware of no subsequent communication from the FTC to any WHR affiliate advising such affiliate that it too was a target of the WHR Investigation or any other investigation being conducted by the FTC.

the course of this investigation and the triviality of the supposed case that Staff has built against WHR by means of that investigation). Wyndham is therefore confident that the CID would be quashed in its entirety if the matter were to be litigated.

Nonetheless, consistent with its two-year history of cooperation with the WHR Investigation, Wyndham sought to negotiate modifications to the CID that would prevent it from unduly burdening Wyndham while at the same time still giving Staff plenty of ability to obtain from Wyndham any additional discovery that it might genuinely need to complete the WHR Investigation. Specifically, in the meet-and-confer conference relative to the CID that Wyndham and Staff conducted on January 6, 2012 pursuant to 16 C.F.R. § 2.7(d)(2),⁸ Wyndham proposed that the CID be modified as follows:

- ***First***, with WHR’s having already fully responded to no fewer than 51 interrogatories and 29 document requests during the course of the WHR Investigation, Wyndham proposed that the CID be limited to posing up to 10 more interrogatories and 10 more document requests—an approach that would still leave Staff with an aggregate total of 61 interrogatories and 39 document requests during the course of the WHR Investigation, as compared to the 25 interrogatory cap that applies to all federal cases under the Federal Rules of Civil Procedure.
- ***Second***, Wyndham proposed that the up-to-10 additional interrogatories and additional document requests that would be permitted under Wyndham’s proposal be drafted by Staff so as to cure the three drafting defects that infect most of the CID’s current discovery requests. Wyndham thus proposed that any additional interrogatories and any additional targeted document requests be drafted so as to:
 - avoid duplicating discovery requests Staff had previously made and WHR had already responded to;
 - exclude from their scope documents and information that have nothing whatever to do with the WHR Investigation, such as documents and information relative to the information security practices of WHR’s affiliates and service providers; and
 - address the extreme breadth of most of the CID’s current interrogatories and targeted document requests, and the extreme level of detail demanded by those interrogatories and targeted document requests, by instead seeking with precision particular documents and information that Staff has not previously requested, that reasonably relates to some specific concern that has arisen during the WHR Investigation, and that would reasonably be expected to be readily accessible to Wyndham.
- ***Third***, in regard to any “all documents requests” that Staff might include in the

⁸ The statement required by § 2.7(d)(2) is attached hereto as Exhibit 9.

revised CID, Wyndham proposed that Staff identify up to three additional custodians whose documents would be reviewed in order to locate documents responsive to any such requests.

See Letter of Douglas H. Meal to Kristin Krause Cohen, January 8, 2012, attached hereto as Exhibit 10 (memorializing proposal made by Wyndham during the meet-and-confer conference).⁹

Staff did not respond to Wyndham's January 6 proposal until January 12, 2012. See Letter of Kristin Krause Cohen to Douglas H. Meal and Lydia Parnes, January 12, 2012, attached hereto as Exhibit 11. Staff's response rejected virtually all of Wyndham's proposal, but invited further discussions in an effort to resolve Wyndham's objections to the CID. The next day, Wyndham responded by expressing a willingness to engage in further discussions of that sort, but noted that with Wyndham's deadline for filing a petition to quash the CID being now just a week away, Wyndham would be fully occupied during that week in preparing its petition, so further discussions relative to Wyndham's objections to the CID would have to occur after the petition was filed unless Staff were willing to extend that deadline so as to enable such discussions to occur immediately. Staff did not reply to Wyndham's communication, leaving Wyndham with no choice but to complete and file this petition.

ARGUMENT

Although the FTC has broad statutory authority under 15 U.S.C. § 45(a) to investigate practices that it determines may be deceptive or unfair when used in the course of trade, it is well established that FTC's subpoena power is not unfettered. Although Congress has provided the FTC with authority to conduct reasonable investigations through the use of CIDs, those CIDs are not self-enforcing, and federal courts stand as a safeguard against abusive CIDs. See, e.g., *SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1024 (D.C. Cir. 1978), *cert. denied*, 439 U.S. 1071 (1979) ("The federal courts stand guard, of course, against abuses of their subpoena-enforcement processes....") (citing *U.S. v. Powell*, 379 U.S. 48, 58 (1964) and *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 216 (1946)); *D.R. Horton, Inc. v. Jon Leibowitz, Chairman*, No. 4:10-CV-547-A, 2010 WL 4630210, at *2 (N.D. Tex. Nov. 3, 2010) ("As the government notes in its motion documents, the CID is not self-executing, and may only be enforced by a district court in an enforcement proceeding. . .").

⁹ Wyndham's January 8 letter also noted that, while not addressed in the January 6 teleconference, Wyndham generally objects to the CID insofar as it defines "personal information" to include employee information; insofar as it requires a privilege log (at least one as detailed as set forth in the CID); insofar as it defines terms such as "document", "identify", and "relating to" to have something other than their standard English meanings; insofar as it purports to treat documents as being in Wyndham's possession, custody, and control that would not be treated as such under the Federal Rules of Civil Procedure; insofar as it purports to impose a search obligation on Wyndham beyond the search obligation that would be imposed under the Federal Rules of Civil Procedure; insofar as it imposes protocols for document and information production that are different from those protocols that have been followed by WHR thus far in the course of the investigation; insofar as it is addressed to Wyndham Worldwide Corporation rather than to WHR; insofar as it purports to allow only 30 days for compliance; and insofar as it treats the relevant time period as extending beyond May 2010. Wyndham accordingly stated that its proposal should be read to include a request that these aspects of the CID be redrafted as well.

The Supreme Court, in *U.S. v. Morton Salt Co.*, 338 U.S. 632 (1950), established the standard for determining whether a CID should be quashed or limited. Although the Court enforced the decree that was before it in that particular case, it recognized that “a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power.” *Id.* at 652. Accordingly, the Court instructed that agency subpoenas or CIDs should not be enforced if they demand information that is: (a) not “within the authority of the agency,” (b) “too indefinite,” or (c) not “reasonably relevant” to the inquiry. *Id.* This standard has been consistently applied by the courts. *See, e.g., SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512, 514 (10th Cir. 1980) (citing *Morton Salt*, 338 U.S. at 653) (confirming that “[t]o obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”); *Arthur Young & Co.*, 584 F.2d at 1030-31 (noting that the subpoena request must “not [be] so overbroad as to reach into areas [that] are irrelevant or immaterial” and that specifications must not exceed the purpose of the relevant inquiry) (internal quotation marks and citation omitted).

In applying the *Morton Salt* standard, the costs and burdens imposed on the target of a CID also must be considered. *See, e.g., FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977) (a party challenging a subpoena can do so by showing the compliance costs are overly burdensome or unreasonable); *Phoenix Bd. Of Realtors, Inc. v. Dep’t of Justice*, 521 F. Supp. 828, 832 (D. Ariz. 1981) (the government should negotiate to narrow scope of a CID when compliance may be overly burdensome). Thus, administrative agencies may not use their subpoena powers to go on fishing expeditions. *FDIC v. Garner*, 126 F.3d 1138, 1146 (9th Cir. 1997); *FTC v. Nat’l Claims Serv., Inc.*, No. S. 98-283, 1999 WL 819640, at * 1 (E.D. Cal. Feb. 9, 1999). *See also* S. Rep. No. 96-500 at 1105, 96th Congress 1st Session (1979) (“The FTC’s broad investigatory powers have been retained but modified to prevent fishing expeditions undertaken merely to satisfy its ‘official curiosity.’”). “It is contrary to the first principles of justice to allow a search through all the respondents’ records, relevant or irrelevant, in the hope that something will turn up.” *FTC v. Am. Tobacco Co.*, 264 U.S. 298, 306 (1924).

Upon applying the *Morton Salt* standard to the CID at issue here, there can be no doubt that the CID must be quashed. To begin with, for a variety of reasons the CID is invalid. *See* Part I below. In addition, the CID is wildly indefinite in numerous respects, is not reasonably relevant to the WHR Investigation in numerous other respects, is for the most part nothing more than a fishing expedition, and—perhaps worst of all—would impose an enormous burden on Wyndham that cannot possibly be justified when one considers the voluminous amount of information and documents that WHR has already provided to Staff, the paucity of the evidentiary record that the WHR Investigation has generated regarding possible Section 5 violations on the part of WHR, and the triviality of the one (and only) Section 5 violation that Staff believes (wrongly) the WHR Investigation has thus far uncovered. *See* Part II below.

I. THE CID IS INVALID

For a variety of reasons, the CID is invalid and, accordingly, must be quashed under *Morton Salt*. To begin with, the CID is not predicated on a Commission-adopted investigational resolution of the sort expressly required both by statute and by the FTC’s own regulations. *See*

Part I.A below. Second, issuance of the CID was not predicated on the showing of need for compulsory process that is a necessary prerequisite for any use of compulsory process in an FTC investigation. *See* Part I.B below. Third, in issuing the CID the FTC did not meet its obligation, under its own regulations, to advise Wyndham in the CID itself of the purpose and scope of the investigation, the nature of the Wyndham conduct believed by Staff to have violated Section 5, and the legal theory supporting Staff’s belief. *See* Part I.C below. Fourth, the sequence of events leading up to the issuance of the CID leaves no doubt that it was issued for an improper purpose, which in and of itself invalidates the CID. *See* Part I.D below. Finally, because Staff has no authority to expand the WHR Investigation into WHR’s information security practices regarding employee (rather than consumer) data, or into the information security practices of WHR’s affiliates or service providers, the CID is invalid insofar as it seeks information and documents relative to such security practices. For each, and all, of these reasons, the CID should be quashed.

A. The CID is Not Predicated on a Proper Investigational Resolution

The statutory and regulatory regime governing FTC CIDs expressly provides that a Commissioner may issue a CID *only* as part of an existing investigation with respect to which a resolution authorizing the use of compulsory process in *that* investigation has previously been adopted by the full Commission. The governing statute (Section 20(i) of the FTCA) reads as follows in relevant part:

Notwithstanding any other provision of law, the Commission shall have no authority to issue a subpoena or make a demand for information . . . unless such subpoena or demand for information is signed by a Commissioner *acting pursuant to a Commission resolution*.

15 U.S.C. § 57b-1(i) (emphasis added). Part 2 of Subchapter A of the Commission’s own regulations (the “Rules of Practice”) expressly incorporate this statutory requirement by dictating that “[t]he Commission or any member thereof may, *pursuant to a Commission resolution*, issue a subpoena or civil investigative demand.” 16 C.F.R. § 2.7 (emphasis added). In this regard, the Rules of Practice make clear not only that a CID is only valid if predicated on a Commission-adopted investigational resolution authorizing the use of compulsory process in the investigation in question, but also that a Commission-adopted investigational resolution is only valid if it is adopted as part of an existing FTC investigation of a particular matter, and even then its validity extends *only* to that particular investigation. “[T]he Commission may, *in any matter under investigation* adopt a resolution authorizing the use of any or all of the compulsory processes provided for by law.” 16 C.F.R. § 2.4 (emphasis added). Here, then, the CID is invalid, and must be quashed, unless subsequent to the commencement of the WHR Investigation the full Commission adopted an investigational resolution approving the use of compulsory process in the WHR Investigation.

It is indisputable that the full Commission has never adopted any such resolution in regard to the WHR Investigation. This is made clear by the CID itself, which points to an FTC resolution dated January 3, 2008 as being the Commission-adopted resolution that ostensibly satisfies Section 20(i) of the FTCA and Sections 2.4 and 2.7 of the Rules of Practice in regard to the CID. *See* FTC Resolution No. P954807 (Jan. 3, 2008) (the “January 2008 Resolution”),

which is included in the CID (Exhibit 1 hereto) as an attachment. However, whatever FTC investigation may have been the subject of the January 2008 Resolution, that investigation certainly *was not* the WHR Investigation. The January 2008 Resolution nowhere even makes mention of the WHR Investigation, or of the Intrusions, or even of Wyndham. Nor could it have done so, for the first Intrusion did not even begin until June 2008, six months *after* the January 2008 Resolution was approved by the Commission. As of January 2008, then, there was nothing for the FTC to investigate in regard to WHR's information security practices. Indeed, the WHR Investigation was not commenced until 2010, as shown by the WHR Investigation's seven-digit identification number (1023142). Accordingly, the Commission's adoption of the January 2008 Resolution obviously had nothing to do with the WHR Investigation, and the investigation of WHR's information security practices referenced in the Access Letter (i.e., the WHR Investigation, which according to page 1 of the Access Letter was prompted by the Intrusions) obviously has to be a *different* investigation from the investigation referenced in the January 2008 Resolution. That being the case, the January 2008 resolution does not, and cannot, satisfy the statutory and regulatory requirement that the CID be predicated on a Commission-adopted investigational resolution approving the use of compulsory process in the WHR Investigation.

Wyndham anticipates that Staff will attempt to defend the absence of any resolution adopted by the Commission that references the WHR Investigation by arguing that Section 20(i) of the FTCA and Sections 2.4 and 2.7 of the Rules of Practice can be satisfied, in regard to any given CID, not only by a Commission-adopted resolution specifically addressing the particular investigation that is the subject of the CID, but also by a generic resolution by which the Commission purports to approve the use of compulsory process in Staff investigations of a certain general type, including Staff investigations that at the time of the resolution have not yet been commenced or even conceived of by Staff, but nonetheless are of the general type described in the resolution. In advancing such an argument, Staff will likely point to Section 3.3.6.7.4 of the FTC Operating Manual (the "Operating Manual"), in which the FTC takes the position that the "investigational resolution" requirement embedded in Section 20(i) and Sections 2.4 and 2.7 of the Rules of Practice can be satisfied not only by either a "special resolution" that specifically references the particular Staff investigation and company to which the CID in question relates or an "omnibus resolution" that authorizes an investigation having a particular industry focus rather than a particular company focus,¹⁰ but also by what the Operating Manual defines as a "blanket resolution." Any argument by Staff that the January 2008 Resolution constitutes a "blanket resolution" within the meaning of Section 3.3.6.7.4.3 of the Operating Manual¹¹ and, as such, satisfies the investigational resolution requirement in regard to the CID, would be incorrect for two separate reasons.

First, neither Section 20(i) of the FTCA nor Sections 2.4 and 2.7 of the Rules of Practice can be read to permit the investigational resolution requirement (i.e., the requirement that any CID be predicated on an investigational resolution approved by the full Commission) to be

¹⁰ An "omnibus resolution" is geared toward "an industrywide investigation" into certain "industry conduct or practices." Operating Manual, § 3.3.6.7.4.2. Nothing in the January 2008 Resolution describes the investigation authorized thereby as having an industry focus.

¹¹ As defined in the Operating Manual, when a "blanket resolution" is used to satisfy the investigational resolution requirement, "the investigation is ordinarily directed at certain types of practices rather than specific industries." Operating Manual, § 3.3.6.7.4.3.

satisfied by means of a resolution that does not even *mention* (much less authorize the use of compulsory process in) the particular investigation in which the CID was issued. To begin with, such a reading flies in the face of the unambiguous language of these provisions themselves, which language expressly states that the Commission can only adopt a resolution authorizing compulsory process “in [a] matter under investigation,” 16 C.F.R. § 2.4—not “in [a] matter that may some day come under investigation.” In addition, reading these provisions to be satisfiable by means of “blanket” investigational resolutions would utterly defeat the legislative purpose behind the investigational resolution requirement. Congress enacted Section 20(i) as part of the Federal Trade Commission Improvements Act of 1980. The Senate Report accompanying that bill makes clear that two key objectives of Section 20(i) were “to limit the practice of the Commission of giving a vague description of the general subject matter of the inquiry” and to ensure that the Commission “take[s] very seriously its obligation to demand information only where the information is not available through other means.” *See* S. Rep. No. 96-500, at 1125, 27. Plainly, there is no way for the Commission to meet these congressional objectives by means of “blanket” investigational resolutions, because the Commission cannot possibly include in a blanket investigational resolution anything more than “a vague description of the general subject matter of the inquiry” and cannot in adopting a blanket resolution give even the slightest consideration (much less “take seriously”) whether the information that any given respondent will be compelled to produce pursuant to the resolution “is not available through other means.” To the contrary, the only way the Commission can meet the congressional objectives that underlie the investigational resolution requirement is if the Commission, when called upon to satisfy its statutory duty to ensure that any use of compulsory process in a Staff investigation must always be predicated on an investigational resolution adopted by the full Commission, discharges that duty by evaluating *the particular investigation in question*. In short, then, to the extent Staff were to oppose Wyndham’s petition to quash by taking the position that the investigational resolution requirement embedded in Section 20(i) can be satisfied by means of a “blanket” investigational resolution, Staff would in effect be taking the position that the Commission is entitled to abdicate the very duty of overseeing Staff investigations that Congress intended to impose on the Commission by means of the investigational resolution requirement.

Second, even if the investigational resolution requirement could theoretically be satisfied in a given case by means of a “blanket” resolution, for several reasons the January 2008 Resolution does not come anywhere close to satisfying what even the FTC acknowledges would be required for a particular blanket resolution to pass muster under Section 20(i) of the FTCA and Sections 2.4 and 2.7 of the Rules of Practice:

- For one thing, even the FTC acknowledges in the Operating Manual that “[b]lanket resolutions have been approved by the Commission in a limited number of instances such as in connection with the issuance of ‘second requests’ under the Hart-Scott-Rodino Act,” and that such resolutions ordinarily contemplate an investigation “directed at certain types of practices.” Operating Manual, § 3.3.6.7.4.3. In that regard, the Operating Manual provides an example of what the FTC considers to be a proper blanket resolution; in that example, the resolution expressly limits the investigation in question to a particular category of practices involving the sale of merchandise by mail that violates not only Section 5 but also an entirely separate statute (namely, 39 U.S.C. § 3009) that prohibits the mailing of unordered merchandise in certain circumstances. *See* Operating Manual, Chapter 3, Illustration 11. In contrast, the January 2008 Resolution contains

nothing more than a *topical* limitation on the investigation with respect to which that resolution purports to authorize the use of compulsory process. *See* January 2008 Resolution (included in Exhibit 1 hereto) (authorizing use of compulsory process in an investigation to determine whether unnamed persons have committed deception- or unfairness-based Section 5 violations “related to consumer privacy and/or data security”). Moreover, that topical limitation really operates as no limitation at all, for in net effect the January 2008 Resolution purports to authorize the Bureau of Consumer Protection’s Division of Privacy and Identity Protection to conduct a five-year investigation of any matter within its jurisdiction, during which investigation it can use compulsory process whenever it feels like doing so. As such, the January 2008 Resolution bears no resemblance at all to the sort of “blanket resolution” that the Operating Manual claims (wrongly) might permissibly be used as the predicate for issuance of a CID.

- The FTC also acknowledges in the Operating Manual that “[i]nvestigational resolutions must adequately set forth the nature and scope of the investigation.” Operating Manual § 3.3.6.7.4.1. This requirement stems from the welter of judicial authority holding that a court may only look to the purpose and scope of an investigation as described in the investigational resolution to determine propriety of a CID predicated on that resolution. *See, e.g., FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1092 (D.C. Cir. 1992) (“[T]he validity of Commission subpoenas is to be measured against the purposes stated in the resolution, and not by reference to extraneous evidence” (citing *FTC v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980))); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977) (“The relevance of the material sought by the FTC must be measured against the scope and purpose of the FTC’s investigation, as set forth in the Commission’s resolution”). The January 2008 Resolution, however, says nothing at all about the nature and scope of the WHR Investigation (nor could it have, since the WHR Investigation was more than two years away from being commenced at the time the January 2008 Resolution was adopted). Accordingly, the January 2008 Resolution does not begin to satisfy the requirement (which even the FTC acknowledges) that an investigational resolution provide sufficient detail regarding the investigation in question to enable a court to determine the relevance to the investigation of the material being sought by the compulsory process in question.
- Finally, by its own express terms the January 2008 Resolution only purports to authorize the issuance of compulsory process in “this investigation” (*see* Exhibit 1 hereto)—i.e., in the investigation that is described in the January 2008 Resolution and that is identified by FTC File No. P954807. *See* Exhibit 1 hereto. Thus, even if the January 2008 Resolution were a sufficient predicate for the use of compulsory process in the investigation described and identified in the January 2008 Resolution, by its own terms the January 2008 Resolution does not purport to authorize the use of compulsory process in any *other* investigation Staff might conduct. In that regard, the CID was issued not in the investigation described and identified in the January 2008 Resolution, but rather in *the WHR Investigation*—i.e., in the investigation that is described in the Access Letter as seeking to determine whether “Wyndham’s [i.e., WHR’s] information security practices comply with Section 5” and that is identified by FTC File No. 1023142. *See* Letter of Kristin Krause Cohen to Lydia Parnes and Douglas H. Meal, dated January 6, 2012, attached hereto as Exhibit 12 (describing the CID as having been issued “in our

investigation related to unauthorized access to the computer network of Wyndham Hotels and Resorts, LLC”). Since by Staff’s own acknowledgment the CID was not issued in the investigation referenced and identified in the January 2008 Resolution, the very terms of the January 2008 Resolution preclude the January 2008 Resolution from serving as a valid predicate for the issuance of the CID. That being the case, and there being no Commission-approved investigational resolution of any kind with respect to *the WHR Investigation*, there is no valid predicate for the CID, whether or not the January 2008 Resolution might be thought to be a valid predicate for compulsory process that might be issued in the investigation referenced in that particular resolution.

In sum, for all the foregoing reasons, the January 2008 Resolution is entirely different from those investigational resolutions that have passed muster in the courts. For example, in *FTC v. O’Connell Assocs., Inc.* 828 F. Supp. 165, 167 & n.1 (E.D.N.Y. 1993), the 1990 investigational resolution on which the FTC’s CIDs were predicated was an omnibus resolution (not a blanket one) authorizing an ongoing investigation into the consumer credit reporting industry, and the tip that the FTC received in 1992 that led to the issuance of the CIDs was generated as part of that *same* investigation. Here, in contrast, there is no suggestion that the CID was issued as part of what the January 2008 Resolution describes as a generic investigation into “consumer privacy and/or data security” violations being conducted by the Bureau of Consumer Protection’s Division of Privacy and Identity Protection over a five-year period. To the contrary, it is undisputed that the CID was issued in an entirely different Staff investigation of one particular company’s information security practices, and that the Commission has never approved an investigational resolution as to *that* investigation. Moreover, even if the CID had been issued in the investigation described in the January 2008 Resolution, permitting that resolution to serve as a valid predicate for the CID would mean that the Commission has the authority to grant the Bureau of Consumer Protection’s Division of Privacy and Identity Protection what amounts to a blank check to utilize compulsory process whenever and wherever it so desires during a five-year period. This reading of Section 20(i) of the FTCA and Sections 2.4 and 2.7 of the Rules of Practice would fly in the face of the language of those provisions, ignore the FTC’s own interpretation of that language, and eviscerate the investigational resolution requirement that Congress put in place precisely to protect against the Commission’s compulsory process authority being used in the abusive fashion that occurred here.

B. The CID Was Not Issued Based on the Required Showing of Need for Compulsory Process to Be Used in the WHR Investigation

As noted above, Section 20(i) of the FTCA expressly prohibits any compulsory process from being issued in an FTC investigation unless (i) the full Commission has adopted an investigational resolution authorizing the use of compulsory process in the context of that particular investigation and (ii) a Commissioner has in turn approved the particular form of compulsory process that Staff is proposing to propound pursuant to that investigational resolution.¹² Congress included Section 20(i) in the Federal Trade Commission Improvements Act of 1980 for the precise purpose of “curtail[ing] the issuance by the Commission of overly

¹² “Notwithstanding any other provision of law, the Commission shall have no authority to issue a subpoena or make a demand for information . . . unless such subpoena or demand for information is signed by a Commissioner acting pursuant to a Commission resolution. The Commission shall not delegate the power conferred by this section to sign subpoenas or demands for information to any other person.” 15 U.S.C. 57b-1(i).

broad subpoenas.” *See* S. REP. NO. 96-500 at 1107. In that regard, Congress made clear that going forward, in a situation where a company had already provided substantial information during the course of an investigation, Congress expected the Commission (i) to seek additional information via compulsory process “only if the [C]ommission determines, after reviewing the initial submission, that more information is required” and (ii) to adhere to “its obligation to demand information [via compulsory process] only where the information is not available through other means.” *Id.* at 1127. Moreover, in order to ensure that the Commission would achieve these congressional objectives, the Senate Report included the following express, and unambiguous, directive to the Commission in regard to the process to be followed by the Commission in satisfying the non-delegable obligations imposed on it under Section 20(i):

[T]he Committee intends that the agency require staff memos to the Commission before a CID is issued to describe with specificity the information needed, the reasons why the information is relevant to the inquiry, and the cost and burden production will impose on target companies. The Committee also intends that the agency require Commission staff to explain why the information is not available through alternative (voluntary) means. The Committee intends that under this new procedure, the Commission will carefully review a subpoena before it is issued. In particular, the Commission should make appropriate use of staggered production schedules to minimize burden and inconvenience.

Id.

The Commission itself recognizes the responsibility it has, under Section 20(i) of the FTCA, to insist that Staff makes a proper showing of justification to the Commission at all steps along the path of compulsory process, from beginning the investigation, to obtaining a resolution that authorizes compulsory process, to acquiring permission to use a specific instance of compulsory process, such as any given CID. Specifically, pursuant to the Operating Manual:

- Staff requests for approval of full investigations are to be made by means of a transmittal memorandum addressed to either the Bureau Director or (where Staff intends for compulsory process to be used in the course of the investigation) the Commission. Operating Manual, § 3.3.5.1.2. The “memorandum requesting approval for full investigation should . . . explain the need for approval of the full investigation, including a discussion of” such factors as “[a] description of the practices and their impact on consumers,” the “[e]xtent of consumer injury inflicted by the practices to be investigated,” “[w]hat forms of relief are contemplated,” and “justification for use of compulsory process.” *Id.* § 3.3.5.1.4.
- Similarly, Staff requests for approval of an investigational resolution are to be submitted in the form of a memorandum addressed to the Commission, which “should include a general statement of the nature of the investigation in addition to the justification for the use of compulsory procedures” as well as “a cost summary.” *Id.* § 3.3.6.7.3. As noted above, under Section 20(i) the Commission is obliged to find the use of compulsory process to be justified “only where the information is not available through other means.” S. REP. NO. 96-500, at 1127. Consistent with that statutory obligation, under the

Operating Manual the only legitimate reasons for requesting authority to use compulsory process that are identified in the Operating Manual are “to avoid delay, to obtain testimony under oath, to obtain evidence from persons who will not or who [S]taff believe will not provide complete information voluntarily, or to prevent destruction or withholding of evidence and preserve the Commission’s legal remedies against any such destruction or withholding.” Operating Manual, § 3.3.6.7.2.

- Finally, when Staff requests that the Commission issue a CID pursuant to an investigational resolution previously adopted by the full Commission, Staff is required to submit the proposed CID to the responsible Commissioner for approval, along with a “justification memorandum” that “should describe with specificity . . . the information needed, the reasons why the information is relevant to the inquiry, and the cost and burden production will impose on target companies.” *Id.* § 3.3.6.7.5.4.

Unfortunately, notwithstanding the Commission’s clear legal duty to approve a Staff request for the issuance of compulsory process in a particular investigation only where the request has been justified by Staff in the manner set forth in the Senate Report and the Operating Manual, here it is beyond dispute that the CID issued without any such justification having been provided by Staff or required either by the Commission when it authorized compulsory process to be used in the WHR Investigation or by the responsible Commissioner when the CID itself was issued:¹³

- To begin with, Staff’s memorandum seeking authorization to institute the WHR Investigation could not have described, and the Commission’s and/or the Bureau Director’s approval of the WHR Investigation’s could not have been based on, any alleged “consumer injury inflicted by the practices to be investigated.” *See id.* § 3.3.5.1.4. As noted above, payment card issuers protect their cardholders from suffering any financial injury by reason of their payment card data being compromised, and payment card data was the only personal information placed at risk of compromise during the Intrusions. *See* page 4 above. That being the case, no substantial consumer injury resulted from the Intrusions, and any claim by Staff or finding by the Bureau Director or the Commission to the contrary would have been clearly wrong.
- Further, Staff’s memorandum seeking issuance of the CID could not have accurately described, and the Commissioner’s issuance of the CID could not have been based on an accurate understanding of, “the reasons why the information is relevant to the inquiry, and the cost and burden production will impose on target companies.” *See id.* § 3.3.6.7.5.4. Indeed, there is simply no way any Commissioner would ever have issued

¹³ Obviously, the clearest way to assess the propriety of Staff’s effort to justify using compulsory process in the course of the WHR Investigation would be by examining the required memoranda by which Staff (i) sought authority to institute the WHR Investigation; (ii) asked that the Commission adopt the investigational resolution on which the CID ostensibly is predicated (i.e., the January 2008 Resolution); and (iii) asked that the Commission issue the CID. Accordingly, by means of a letter dated January 13, 2012, Wyndham asked Staff for copies of the required memoranda (among other documents). *See* Exhibit 13 hereto. By letter dated January 17, 2012, Staff refused to provide the requested memoranda to Wyndham, claiming it had no obligation to do so and that Wyndham had not explained its reason for seeking the memoranda. *See* Exhibit 11 hereto. Wyndham accordingly sent Staff a letter dated January 19, 2012 explaining the obvious relevance of the documents Wyndham had requested. *See* Exhibit 15 hereto. Staff never responded to that letter prior to the deadline for filing Wyndham’s petition to quash the CID.

the CID had he or she appreciated the rampant overbreadth of the CID in making inquiries into the information security practices of WHR's affiliates and service providers, the pervasive duplicativeness of the CID's repeated requests for information and documents that WHR has already provided in its response to the Access Letter and subsequent Staff requests, and the multi-million-dollar financial burden compliance with the CID would place upon Wyndham, on top of the millions of dollars of out-of-pocket costs Wyndham has already incurred in voluntarily cooperating with the WHR Investigation. *See* pages 5-6 above.

- Finally, and most important, any Staff memorandum seeking authorization to use compulsory process in the course of the WHR Investigation, whether submitted in seeking authorization to institute the investigation or adoption of an investigational resolution or issuance of the CID, could not possibly have presented the statutorily required justification for the use of compulsory process. As described above, WHR made exhaustive efforts over sixteen months to comply fully and voluntarily with the numerous discovery requests contained in the Access Letter and in Staff's subsequent communications. Staff has never once suggested that those efforts were in any way inadequate to meet Staff's investigatory objectives. *See* page 6 above. Moreover, Staff never once made any effort to obtain voluntarily from Wyndham any of the information and documents requested by the CID. *See* page 22 above. Given these indisputable facts, no Staff memorandum could have possibly satisfied the Commission's statutory obligation to "require Commission staff to explain why the information [sought by a CID] is not available through alternative (voluntary) means." S. REP. NO. 96-500, at 1127. Certainly nothing has occurred in the course of the WHR Investigation to support any claim by Staff, or any finding by the Commissioner who issued the CID, that issuance of the CID was, in the words of the Operating Manual, necessary so as "to avoid delay, to obtain testimony under oath, to obtain evidence from persons who will not or who [S]taff believe will not provide complete information voluntarily, or to prevent destruction or withholding of evidence and preserve the Commission's legal remedies against any such destruction or withholding." Operating Manual § 3.3.6.7.2.

In sum, there is nothing in the record to justify a finding by the Commission, in deciding Wyndham's instant petition to quash the CID, that issuance of the CID was predicated on a proper showing by the Staff, or a valid finding by the Commissioner who issued the CID, that the statutory and regulatory requirements for use of compulsory process in the WHR Investigation in general, and for issuance of the CID in particular, were satisfied here. With Staff and the Commission both having failed to follow the Commission's own internal procedures in authorizing the use of compulsory process in the WHR Investigation and in issuing the CID, the CID is defective and may not be enforced. *See SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512, 514 (10th Cir. 1980) ("[t]o obtain judicial enforcement of an administrative subpoena, an agency must show that . . . all administrative prerequisites have been met" (citing *United States v. Morton Salt Co.*, 338 U.S. 632 (1950))); *accord SEC v. Wall St. Transcript Corp.*, 422 F.2d 1371, 1375 (2d Cir. 1970).

- C. The CID Does Not Inform WHR and WWC of the Purpose and Scope of the WHR Investigation or of the Nature of the Conduct Constituting Their Alleged Section 5 Violation or of How Section 5 Allegedly Applies to Their Conduct

As noted above, one of the key congressional objectives in enacting the Federal Trade Commission Improvements Act of 1980 was to “limit the practice of the Commission of giving [targets of compulsory process] a vague description of the general subject matter of the inquiry.” *See* S. REP. NO. 96-500, at 1125. In place of that practice, Congress intended that upon passage of the statute “[a] civil investigative demand would have to . . . state the nature of the conduct of the alleged violation under investigation and the law applicable thereto.” *Id.* at 1105. The Senate Report explained that the reason for imposing this obligation on the Commission in connection with issuing a CID was not only to accord basic fairness to the recipient of a CID, but also to ensure that every CID “provides a standard by which relevance may be determined” both by the recipient and by a reviewing court in evaluating the propriety of the CID. *Id.* at 1125. As aptly stated by Congressman Coughlin during the House of Representatives debate on the bill:

We need to protect American business from overbroad investigative subpoenas demanding the production of great quantities of information and documents with no requirement that these demands be relevant to some suspected violation. . . . The Commission’s powers of visitation and subpoena are awesome powers that require reasonable safeguards against abuse. The Senate will soon mark up a bill which would curb this subpoena power by requiring that the Commission specify the conduct they are investigating and why the Commission believes that the conduct violates the law. This would force the Commission to draft narrower and more reasonable subpoenas, and also establish criteria for judicial review of these subpoenas.

125 CONG. REC. 32,458 (1979). Senator Heflin echoed this view on the Senate side:

Too often, the Commission has not seen fit to state clearly what conduct it is investigating—leaving the recipients of its subpoena with no basis on which to question the relevance of anything that might be asked for. When the Committee [sic] states, as it has done on occasion, that its purpose in investigating a company is to see whether that company may have been engaged in acts or practice violating section 5 of the FTC Act, and combines that all-inclusive statement of purpose with broad subpoena specifications, what it will get in response approaches the entire contents of that company's files. This is bad for the respondent and, I think, bad for the Commission as well. For this reason, the real heart of section 12 of the bill is a simple requirement applying to the proposed civil investigative demands, as follows: ‘(2) Each such demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable thereto.’ That requirement, allowing some means of challenging the relevance of what the Commission asks for, would become section 20(c)(2) of the act as amended. . . . If the FTC staff has to define what it is after before it starts, rather than asking for everything, then fighting in court to get it, and later sorting out what it really wants, it is likely to make more actual progress in its investigations. . . . [T]he FTC has had a tendency to waste its own time and money, as well as that of subpoena respondents, by failing to bring its subpoena demands under control.

126 CONG. REC. 2394-96 (1980).

As enacted, the statute included a provision containing virtually the exact wording of the proposed provision described by Senator Heflin during the Senate floor debate of the bill:

Each civil investigative demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.

15 U.S.C. § 57b-1(c)(2). The Rules of Practice take this statutory mandate one step further, stating that “[a]ny person under investigation compelled or requested to furnish information or documentary evidence shall be advised of the purpose and scope of the investigation and of the nature of the conduct constituting the alleged violation which is under investigation and the provisions of law applicable to such violation.” 16 C.F.R. § 2.6. Here, then, the CID must be found invalid, and accordingly must be quashed, unless it somewhere advises Wyndham of (i) the purpose and scope of the WHR Investigation; (ii) the nature of the conduct by Wyndham constituting the alleged violation that is under investigation in the WHR Investigation; and (iii) the provision of law applicable to such violation.

The CID does *none* of these three things. Rather, the entirety of the CID’s effort to meet the Commission’s notice obligations under Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice consisted of the following three words that were included in Section 3 of the CID, entitled “Subject of Investigation”:

“See attached resolution”

See Exhibit 1 hereto, at page 1. The “attached resolution” referenced in Section 3 of the CID is the January 2008 Resolution. Regardless of whether the January 2008 Resolution constitutes a proper investigational resolution under Section 20(i) of the FTCA and Sections 2.4 and 2.7 of the Rules of Practice (and Wyndham strongly believes, for the reasons stated in Part I.A above, that it does not), that resolution in no way, shape, or form meets the entirely separate notice requirements of Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice. To begin with, the January 2008 Resolution does not even mention the WHR Investigation, much less advise Wyndham of the purpose and scope of that investigation. Further, the January 2008 Resolution does not even mention Wyndham, much less advise Wyndham of the nature of the conduct by Wyndham constituting the alleged violation that is under investigation in the WHR Investigation. Finally, while the January 2008 Resolution does reference Section 5 of the FTCA, it nowhere describes how that provision of law is allegedly applicable to any conduct on the part of Wyndham. In short, the January 2008 Resolution provides both Wyndham and a reviewing court with literally *nothing* to go on in trying to assess the relevancy to the WHR Investigation of the CID’s interrogatories and document requests. That being the case, the CID fails utterly to meet the Commission’s notice obligations under Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice.

The inadequacy of the January 2008 Resolution for purposes of satisfying the Commission’s notice obligations under Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice becomes evident when one contrasts the January 2008 Resolution with the omnibus resolution at issue in the *Carter* case. As the court indicated in *Carter*, where a CID

seeks to satisfy Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice by cross-referencing an investigational resolution adopted by the Commission, the investigational resolution has to at least provide a “basis for determining the relevancy of the information demanded.” *See FTC v. Carter*, 636 F.2d at 787-88. The investigational resolution at issue in *Carter* did just that, first by actually referencing the investigation in which the CID in question had been issued (something the January 2008 Resolution did not do and could not have done, given that the CID was not in fact issued in the investigation authorized by the January 2008 Resolution), and then “by identifying the specific conduct under investigation.” *Id.* at 787-88. Moreover, rather than including just a broad topical reference to the conduct under investigation, as is the case in the January 2008 Resolution, the investigational resolution relied upon in *Carter* specified particular conduct in detail, namely “the advertising, promotion, offering for sale, sale, or distribution of cigarettes.” *Id.* at 788. Crucially, the *Carter* court pointed out that the resolution had been adopted (in addition to under Section 5 of the FTCA) under “Section 8(b) of the Cigarette Labelling and Advertising Act,” a far more topically-focused statute than Section 5, so much so that the reference to the statute was “self-expressive of several purposes of this investigation.” *Id.* Otherwise, the Court noted that “Section 5’s prohibition of unfair and deceptive practices . . . standing broadly alone would not serve very specific notice of purpose” such that it needed to be “defined by its relationship to section 8(b)” as well as linked “to the subject matter of the investigation.” *Id.*

In sum, what we have here is a case where, in the words of Senator Heflin, “the Commission has not seen fit to state clearly what conduct it is investigating—leaving the recipients of its [CID] with no basis on which to question the relevance of anything that might be asked for.” 126 CONG. REC. 2394 (1980). Congress took action more than thirty years ago to prohibit the Commission from behaving in this abusive fashion. Wyndham is unaware of any judicial decision in the ensuing 30-plus years approving of an FTC CID where the CID purported to satisfy the Commission’s notice obligations under Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice by cross-referencing an investigational resolution that (i) nowhere even mentions (much less advises the recipient of the purpose and scope of) the investigation in which the CID was issued; (ii) nowhere even identifies the target of the investigation (much less advises the recipient of the nature of the target’s conduct constituting the alleged violation that is under investigation); and (iii) nowhere describes how the provision of law cited in the resolution is allegedly applicable to any conduct on the part of the target. Wyndham therefore is confident that any reviewing court would quash the CID on this ground alone, if for some reason the Commission does not do so itself in response to Wyndham’s instant petition.

D. The CID Was Issued for the Improper Purpose of Either Coercing WHR’s Acceptance of Unlawful Settlement Terms or Engaging in Premature Litigation Discovery (or Both)

A CID should be issued, if at all, only in order to investigate whether the law has been violated. *See, e.g.*, Operating Manual, § 3.3.6.7.5.3. Thus, courts will quash agency demands for information that were “issued for an improper purpose, such as to harass [the recipient] or to put pressure on him to settle . . . or for any other purpose reflecting on the good faith of the particular investigation.” *United Sates v. Powell*, 379 U.S. 48, 58 (1964); *see also FTC v. Bisaro*, 2010 WL 3260042, at *5 (D.D.C. July 13, 2010). Here, as detailed below, the record leaves no doubt

that the CID was issued either for the improper purpose of coercing WHR and its affiliates' acceptance of the unlawful settlement terms being insisted on by Staff, or for the improper purpose of enabling Staff to engage in litigation-related discovery in the guise of "completing" an investigation that by Staff's own admission had already accomplished its investigational objectives—or for both improper purposes. For this separate and independent reason, the CID is invalid and must be quashed.

As detailed earlier in this petition (*see* pages 11-12 above), the CID (i) pervasively duplicates Staff's prior requests for documents and information made during the course of the WHR Investigation; (ii) is patently overbroad in without authority seeking to expand the WHR Investigation at the eleventh hour to WHR's employees, affiliates, and service providers; (iii) is wholly unnecessary given that the WHR Investigation has by Staff's own admission already achieved its investigatory objective; and (iv) is unjustifiably burdensome when one takes into account the vast amount of information WHR has already provided to Staff at huge expense during the sixteen-month course of the WHR Investigation, the enormous costs Wyndham would incur in trying to comply with the CID, and the trivial nature of the Section 5 violation that Staff believes it found after sixteen months of investigating WHR's information security practices. Given these facts, it ought to be obvious to the Commission, and if not it certainly would be obvious to a reviewing court, that the CID in no way represents a good faith attempt by Staff to request of WHR merely whatever minimal additional discovery Staff might at this juncture legitimately believe it needs to complete the WHR Investigation. To the contrary, the Commission should find, and if it does not a reviewing court would find, that the only plausible explanation for the CID's enormous breadth is that it was drafted and served for the improper purpose of coercing WHR and its affiliates into accepting the Staff settlement terms being objected to by WHR—settlement terms that, as demonstrated in the white paper delivered by WHR to Staff on November 21, 2011 (Exhibit 7 hereto), Staff has no lawful basis for seeking to impose on WHR and its affiliates.

In evaluating Staff's true purpose in requesting issuance of the CID, the Commission should (and a reviewing court surely would) note that the CID was served only days after WHR delivered its white paper demonstrating the unlawfulness of the settlement terms being demanded by Staff and objected to by WHR. Moreover, the Commission should (and a reviewing court surely would) find it telling that Staff flatly refused Wyndham's request for a copy of the memorandum Staff was required to prepare for and submit to the responsible Commissioner in requesting issuance of the CID (*see* note 13 above), even though such memorandum is directly relevant to any evaluation by the Commission or a reviewing court of the propriety of Staff's purpose in seeking issuance of the CID. Perhaps more telling still is the fact that even now, two months after the white paper was delivered, Staff has provided WHR with no rebuttal of any sort to the arguments WHR advanced in the white paper as to the unlawfulness of the settlement terms being demanded by Staff. Indeed, to this day Staff's only response to the legal arguments in WHR's white paper has been to seek and obtain issuance of the CID. The message being conveyed by Staff by means of that response could not have been clearer: "Settle on our unlawful terms Wyndham—or else we will crush you with our discovery requests." As Judge Posner said in a recent decision granting an injunction to prevent one party's "threat to turn the screws" using costly discovery, "the pressure on [defendant] to settle on terms advantageous to its opponent will mount up if [opposing] counsel's ambitious program of discovery is allowed to continue." *Thorogood v. Sears, Roebuck and Co.*, 624 F.3d 842, 850

(7th Cir. 2010), *vacated and remanded on other grounds*, 131 S. Ct. 3060 (2011). Here then, just as Judge Posner did in *Thorogood*, the Commission should block the “ambitious program of discovery” reflected in Staff’s CID and thereby put an end to Staff’s blatant attempt to “turn the [settlement] screws” on Wyndham by seeking and obtaining issuance of the CID.

What makes Wyndham’s improper-purpose argument for quashing the CID even more compelling is the powerful record evidence that Staff sought issuance of the CID not only for the improper purpose of coercing Wyndham to accept an unlawful settlement, but also (in the event Wyndham did not accept Staff’s unlawful settlement terms) for the additional improper purpose of enabling Staff to obtain litigation-related discovery from Wyndham without in so doing being subject to the rules and limitations that are supposed to govern such discovery. As described earlier in this petition (*see* pages 7-8 above), by the time the CID was issued, Staff had already advised WHR that Staff believed, based on the results of the WHR Investigation, that WHR’s information security practices violated Section 5. Moreover, based on that belief, Staff was prepared to recommend corrective action to the Commission in the form of a consent agreement. Indeed, Staff had already provided WHR with the consent agreement it was prepared to recommend to the Commission and a proposed complaint alleging a violation of Section 5 on the part of WHR and certain of its affiliates. Any investigation that has reached a point at which Staff believes it has found a Section 5 violation and is ready to recommend corrective action to the Commission is by definition “complete,” because once an investigation reaches that point Staff by definition has no need for any further information in order to conclude the investigatory phase of the case (*see* Operating Manual § 1.3.4.4) and proceed with the next phase of the case. Given that by the time the CID was issued Staff plainly had no need for further discovery from WHR in order to complete the investigatory phase of the case and move forward with the corrective action phase, the second obvious explanation for Staff’s having sought and obtained issuance of the CID is that, in the event Wyndham resisted Staff’s coercive settlement demands, Staff hoped to use the CID to obtain discovery to be used by Staff in litigating against Wyndham once the Proposed Complaint was filed. But discovery of *that* sort is supposed to be sought and obtained by Staff not in the guise of completing an already-completed investigation, but rather under and subject to the Commission’s rules for adjudicative proceedings, as authorized by an Administrative Law Judge. For this additional reason, then, the Commission should find (and if it does not a reviewing court would find) that the CID was sought and obtained by Staff for an improper purpose and as a consequence must be quashed.

The law is clear that Staff may not abuse the judicial process by seeking and obtaining issuance of a CID for “illicit purposes.” *SEC v. Wheeling-Pittsburgh Steel Corp.*, 648 F.2d 118, 126 (3d Cir. 1981). Because Staff did precisely that here, the Commission should quash the CID.

- E. Because Staff Has No Authority to Investigate Employee Injuries or the Information Security Practices of WHR’s Affiliates and Service Providers, the CID Is Invalid Insofar As It Seeks Information and Documents Relative to Those Matters

The permissible scope of a CID is no broader than the permissible scope of the Staff investigation in which the CID is issued. The permissible scope of a Staff investigation depends,

in turn, on (i) how the scope of the investigation was defined by the Commission or the Bureau Director upon approving either the institution of or an expansion of the investigation and (ii) whether the scope of the investigation, as approved by the Commission or the Bureau Director, exceeds the Commission's investigatory jurisdiction as provided by Congress under the FTCA. Here, the scope of the CID exceeds the permissible scope of the WHR Investigation in two significant respects. First, insofar as the CID seeks discovery regarding WHR and its affiliates' handling of data of their employees¹⁴ and discovery relative to the information security practices of WHR's affiliates and service providers,¹⁵ the CID exceeds the bounds of the WHR Investigation as defined by the Commission and/or the Bureau Director. *See* Part I.E.1 below. Second, whether or not by seeking such information the CID exceeds the bounds of the WHR Investigation as defined by the Commission and/or the Bureau Director, the CID certainly exceeds the bounds of the FTC's investigatory jurisdiction as conferred by Congress insofar as it seeks information regarding WHR and its affiliates' handling of data of their employees. *See* Part I.E.2 below. The CID is therefore invalid, and must be quashed, both insofar as it seeks information and/or documents relative to how WHR and its affiliates handle employee data and also insofar as it seeks information relative to the information security practices of WHR's affiliates and service providers.

1. Staff Has Not Been Authorized to Investigate Employee Injuries or the Information Security Practices of WHR's Affiliates and Service Providers

As discussed in Part I.C above, under Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice, Wyndham, the Commission, and a reviewing court are all supposed to be able to look at the CID itself in order to determine how the scope of the WHR Investigation was defined by the Commission and/or the Bureau Director upon approving either the institution or an expansion of the WHR Investigation. Unfortunately, as shown in Part I.C above, here the CID fails to comply with Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice, in that it fails to provide any description of the scope of the WHR Investigation (a circumstance that in and of itself requires the CID to be quashed). Here, then, thanks to the CID's violation of Section 20(c)(2) of the FTCA and Section 2.6 of the Rules of Practice, neither Wyndham nor the Commission nor a reviewing court can determine the authorized scope of the WHR Investigation, and hence the permissible scope of the CID, by reference to the CID itself.

That being the case, the next best place to look in order to determine how the scope of the WHR Investigation was defined by the Commission and/or the Bureau Director upon approving either the institution or an expansion of the WHR Investigation would be to review any

¹⁴ The CID seeks such information by defining "personal information"—a term that is incorporated extensively into the document requests and interrogatories—to include information about the *employees* of WHR and its affiliates: "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." *See* Exhibit 1 hereto, Definition T.

¹⁵ Many of the CID's interrogatories and document requests address in whole or in part the information security practices of Wyndham's service providers (see Exhibit 1 hereto, Interrogatory 14 and Document Request 8) or affiliates (see Exhibit 1 hereto, Interrogatories 5, 6, 7, 8, 12, 13, 14, 16, 17, 18, 19, 20, and 21, and Document Requests 3, 6, 7, 8, 9, 10, 12, 13, and 16).

documents by which Staff requested, and the Commission and/or the Bureau Director then granted, Staff the authority first to institute and later to expand the WHR Investigation. Thus, during the course of preparing its instant petition to quash, Wyndham asked Staff to provide Wyndham with these very documents. *See* Exhibit 13 hereto. Staff refused to do so, however, even after Wyndham detailed its reasons for requesting those documents. *See* Exhibits 14 and 15 hereto. Thus, while Wyndham is confident that a reviewing court would order Staff to produce those documents to Wyndham in the event the Commission were ever to seek judicial enforcement of the CID, at least for now the documents by which Staff requested that it be given authority, and the Commission and/or the Bureau Director granted Staff authority, first to institute and later to expand the WHR Investigation are not available to assist in determining how the scope of the WHR Investigation was defined by the Commission and/or the Bureau Director.

With Staff having failed to include any description of the scope of the WHR Investigation in the CID and having refused to provide the internal Commission documents that would operate to define the authorized scope of the WHR Investigation, Wyndham is aware of one and only one document that both is currently available for review and purports to describe the authorized scope of the WHR Investigation: the Access Letter. According to the very first sentence of the Access Letter, Staff was “conducting a non-public investigation into *Wyndham Hotels and Resorts, LLC’s* [defined by the Access Letter as “Wyndham”] compliance with federal laws governing information security.” Exhibit 3 hereto at page 1 (emphasis added). The Access Letter explained in its next sentence that the concern giving rise to the investigation was that “sensitive personal information (including credit card information) of *Wyndham’s customers* was obtained from Wyndham’s computer networks by unauthorized individuals.” *Id.* (emphasis added). Thus, according to the Access Letter’s third sentence, Staff was seeking “to determine whether *Wyndham’s* [i.e., WHR’s] *information security practices* comply with Section 5 of the Federal Trade Commission Act.” *Id.* (emphasis added).

In other words, according to Staff’s own description of the WHR Investigation as set forth in the first three sentences of the Access Letter, the investigation Staff had been authorized to conduct involved *WHR’s* information security practices and *WHR’s* compliance with Section 5—not the information security practices or the compliance with Section 5 of WHR’s affiliates or WHR’s service providers. Moreover, per the Access Letter the focal point of the investigation was WHR’s alleged failure to protect personal information of WHR’s *customers*—not an alleged failure by WHR to protect personal information of WHR’s *employees*. Further, at no point since its receipt of the Access Letter has WHR received any documentation from Staff advising WHR that the WHR Investigation had been expanded, beyond the scope set forth in the Access Letter, to extend to the protection of employee data by WHR or its affiliates or to the information security practices of WHR’s affiliates and/or service providers. Nor has WWC or any other WHR affiliate ever received any documentation from the Commission as required by Section 3.3.6.1 of the Operating Manual notifying such entity that it had become a proposed respondent in the WHR Investigation.

In short, the documentary record that is available for review as to how the scope of the WHR Investigation has been defined by the Commission and/or the Bureau Director compels the conclusion that Staff has *never* been authorized by either the Commission or the Bureau Director to investigate the protection of employee data by WHR and its affiliates or to investigate the

information security practices of WHR’s affiliates and/or service providers. The conclusion that the authorized scope of the WHR Investigation *does not* extend to such matters in turn compels the conclusion that the permissible scope of the CID *cannot* extend to such matters. Accordingly, the CID is necessarily invalid, and must be quashed, insofar as it seeks information and/or documents relative to how WHR and its affiliates handle employee data and also insofar as it seeks information relative to the information security practices of WHR’s affiliates and service providers.

2. The FTC In Any Event Has No Jurisdiction to Investigate Employee Injuries

To establish an unfairness-based Section 5 violation, the FTC must show that the respondent’s conduct “causes or is likely to cause substantial injury to *consumers* which is not reasonably avoidable by *consumers* themselves and not outweighed by countervailing benefits to *consumers* or to competition.” 15 U.S.C. § 45(n) (emphasis added). Likewise, conduct is deceptive under Section 5 only if “first, there is a representation, omission, or practice that, second, is likely to mislead *consumers* acting reasonably under the circumstances, and third, the representation, omission, or practice is material.” *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009) (emphasis added) (quotations omitted). By definition, then, the FTC’s investigatory jurisdiction extends only to acts or practices that affect people in their capacity as “consumers.”

To be a “consumer” under the FTCA, a person must be a purchaser or user of goods or services. The common meaning of the term imposes this requirement. *See* BLACK’S LAW DICTIONARY (9th ed. 2009) (consumer is “[a] person who buys goods or services for personal, family, or household use, with no intention of resale; a natural person who uses products for personal rather than business purposes”); Webster’s II New College Dictionary (3d ed. 2005) (consumer is a “person who acquires goods or services : Buyer”).¹⁶ Likewise, the FTC has advocated this limitation on the definition of “consumer” in federal court. Brief of FTC in *FTC v. IFC Credit Corp.*, 2007 WL 5193297 (N.D. Ill. filed July 25, 2007) (“consumer,” as used in the FTC Act, means a “*purchaser or user of goods or services*”) (emphasis added). Employees serve their employers rather than purchase or use their employers’ goods or services, and thus are not “consumers” of their employers’ goods or services under the statute.

While some recent FTC data security consent decrees have defined “consumers” to include “employees” “[f]or the purpose of” the decree (*see, e.g., In re Ceridian Corp.*, No. C-4325, 2011 WL 2487159, at *3 (F.T.C. June 8, 2011) (consent order)), these decrees do not support the proposition that employees are “consumers” for purposes of the FTCA. First, as the FTC itself has admitted in federal court, consent decrees affect the legal rights *only* of the parties who sign them. Brief of FTC in *POM Wonderful LLC v. FTC*, No. 10-1539, at 11-12 (D.D.C. filed Nov. 16, 2010). They do not serve as precedent or otherwise define rights under Section 5; to the contrary, they often impose requirements that are “more restrictive” than those imposed by the FTCA. *Id.* Because the proper purpose of a CID is to determine whether Section 5 has been

¹⁶ “Courts properly assume, absent sufficient indication to the contrary, that Congress intends the words in its enactments to carry their ordinary, contemporary, common meaning.” *Pioneer Investment Svcs. Co. v. Brunswick Associates Ltd. Partnership*, 507 U.S. 380, 388 (1993) (internal quotation omitted). Section 5 does not define the term “consumer.”

violated, Section 5, not consent orders, defines the CID's proper scope. Second, to the extent these consent orders could somehow inform an interpretation of Section 5—which they could not—they in fact show that employees are *not* consumers within the meaning of the FTCA. By defining “consumers” to include “employees” “*for the purpose of*” a consent order, they, like the definition of “personal information” contained in the CID (*see* note 9 above), effectively concede that for *other* purposes—i.e., under the standard meaning that applies under Section 5—employees are *not* consumers. Otherwise, there would be no need to artificially add “employees” to the definition.

Because employees are not “consumers” for purposes of the FTCA, the FTC has no investigatory jurisdiction with regard to acts or practices that affect persons in their capacities as employees. Given the FTC's lack of any basis to assert investigatory jurisdiction over conduct respecting employees, the CID's pervasive effort to obtain information and/or documents relative to how WHR and its affiliates handle employee data (*see* note 9 above) would be invalid even if the Commission and/or the Bureau Director had purported to authorize the WHR Investigation to extend to such matters (which, as discussed in Part I.E.1 above, evidently did not occur). For this reason as well, then, Staff's attempt to use the CID to investigate to how WHR and its affiliates handle employee data (which would seem to be a rather transparent, and feeble, effort by Staff to circumvent Staff's clear inability to show any substantial *consumer* injury as a result of the Intrusions, *see* page 3 above) is invalid. The CID must therefore be quashed to the extent it seeks information and/or documents relative to how WHR and its affiliates handle employee data.¹⁷

II. THE CID MUST BE QUASHED BECAUSE IT IS OVERBROAD, UNDULY BURDENSOME, AND TOO INDEFINITE

Even if the CID were a valid exercise of FTC authority (which, as shown in Part I above, it is not), and the CID nonetheless must be quashed because it is overbroad, unduly burdensome, and too indefinite. First, the CID is overbroad throughout because request after request seeks information and/or documents not reasonably relevant to the WHR Investigation and thus constitutes a fishing expedition by Staff regarding activities and entities that Staff has no reason to believe violated Section 5. *See* Part II.A below. Second, the CID should be quashed in its entirety, or at a minimum should be drastically limited, on the basis that compliance with the CID as drafted would impose a burden on Wyndham that is both hugely costly and utterly disproportionate in scope to the trivial nature of the Section 5 violation that Staff believes it has found in this case, particularly when one takes into account the enormous amount of information and documents WHR has already voluntarily provided in the course of the WHR Investigation and the enormous expense WHR has incurred in so doing. *See* Part II.B below. Third, virtually all of the requests contained in the CID are too indefinite to constitute valid demands. *See* Part

¹⁷ By a letter dated January 12, 2012, *see* Exhibit 11 hereto, Staff stated that it would “recommend to our Associate Director that the CID be modified to include in the definition of personal information only customer information.” No such modified CID was ever served by Staff prior to the deadline for filing Wyndham's petition to quash, however, nor did the Associate Director agree to modify the CID. Thus, Wyndham was left with no choice but to include in this petition its objections to the CID's effort to obtain information and/or documents relative to how WHR and its affiliates handle employee data.

II.C below.¹⁸

A. The CID Is Pervasively Overbroad Because Request After Request Seeks Information Not Reasonably Related to the WHR Investigation

An agency subpoena or CID will not be enforced if it demands information that is not “reasonably relevant” to the inquiry. *U.S. v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (citing relevance as one of three bases for quashing CID). In this case, every single one of the 89 interrogatories and 38 document requests contained in the CID seeks information or documents that are well beyond the scope of the WHR Investigation and/or are not reasonably designed to discover whether WHR violated Section 5. Most notably, many of the requests seek information or documents regarding information security practices of WHR’s corporate affiliates WWC, WHM, and WHG¹⁹ despite the fact that Staff has not pointed (and cannot point) to a shred of evidence indicating that any of these entities violated Section 5 or that any of their networks suffered from information security deficiencies. In fact, Staff’s sole argument in defense of the requests addressed to the information security practices of WHR’s affiliates is that WWC and WHG are relevant because they provided information technology and security services to WHR and WHM is relevant because it provided information security services to the managed Wyndham-branded hotels. *See* Exhibit 11 at 2 (Staff letter noting that WHR’s affiliates are relevant because information security services were provided to WHR by WHG and later by WWC, and to the managed Wyndham-branded hotels by WHM, but failing to state any reason why information or documents related to the separate information security programs of these entities themselves, and unrelated to information security at WHR or the Wyndham-branded hotels, are relevant to the WHR Investigation). Wyndham has never contested the relevance of documents or information in the possession of WHR’s affiliates to the extent such documents or information relate to information security at WHR or the Wyndham-branded hotels. Indeed, WHR has already produced over one million pages of documents from custodians employed by WWC and WHG related to information security at WHR. WHR does contest, however, the relevance to the WHR Investigation of documents or information that has nothing to do with information security at WHR or the Wyndham-branded hotels and instead relates only to information security at WWC, WHG, or WHM. Staff has offered no rationale for the CID’s demand for documents and information of *that* sort. *See* Exhibit 11. Accordingly, the portions of the CID that seek discovery regarding information security practices at WWC, WHG, and WHM that do not involve WHR’s or the Wyndham-branded hotels’ information security should be stricken.

The CID is overly broad in several material respects beyond the requests that target WHR’s affiliates. For example, the CID seeks documents generated during, and information relative to, the period from January 1, 2008 to present, *see* Exhibit 1, Instruction C, despite the fact that WHR had fully remediated the security incidents experienced at the Wyndham-branded hotels by May of 2010. Staff has no reason to believe that documents generated during, or information relative to, the period between May of 2010 and December of 2011 would be

¹⁸ Wyndham hereby incorporates each of the objections stated in Exhibit 16 into this Petition.

¹⁹ *See* Exhibit x hereto, Interrogatories 5, 6, 7, 8, 12, 13, 14, 16, 17, 18, 19, 20, and 21, and Document Requests 3, 6, 7, 8, 9, 10, 12, 13, and 16.

reasonably likely to shed light on WHR's information security practices at the time of the Intrusions (the first of which began in June 2008 and the last of which ended in January 2010). This Instruction therefore should be modified. The CID also, without any basis, defines "personal information" to include information other than the type that was allegedly placed at risk of compromise during the Intrusions and/or information that is beyond the FTC's statutory jurisdiction (such as "employees" information). *See* Exhibit 1, Definition T. This definition thus likewise should be modified. Various other requests in the CID seek information that could not possibly relate to whether WHR's information security practices violated Section 5, such as for example: the dates on which the Wyndham-franchised and managed hotels entered into franchise and management agreements with WHR (Interrogatory 1), the identity of the members of the Board of Directors of WHR and each of its affiliates and the length of time he or she has served in such a role (Interrogatory 22), and the process that WHR's quality assurance program uses to assess the Wyndham-branded hotels' compliance with their contractual obligations (Document Request 14). All of these overbroad requests should be stricken.

With respect to those of the CID's requests that at least facially relate to WHR's information security practices, the CID for the most part appears to be an attempt by Staff to conduct a fishing expedition into every imaginable aspect of those practices, rather than a targeted inquiry into whatever particular aspect of those practices is of concern to Staff based on the sixteen months of investigatory work Staff has already done in this case. For example, as drafted Interrogatory 12 purports to require WHR to describe in detail each and every aspect of any and all information security measures that WHR had in place at any time during the last four years, including the date on which each and every such aspect was implemented, each and every assessment, test, evaluation, monitoring action, or change that was made of or to any such aspect during such period, and the date of every such assessment, test, monitoring action, or change. No effort is made in this interrogatory to zero in on any particular aspect of WHR's information security that Staff might have concerns about based on its investigation to date. Similarly, Interrogatory 14 and Document Request 6 and 8 seek information and documents regarding any and all "Service Providers" who were allowed access to personal information relating to WHR's customers and any and all steps taken by WHR to secure this access, even though the forensic reports produced to Staff regarding the Intrusions do not indicate that any of the Intrusions involved any personal information held by any Service Provider or any failure on the part of WHR to adequately screen or manage a Service Provider. Again, no effort is made in this request to zero in on the activities of whatever particular Service Providers are of concern to Staff based on the results of the WHR Investigation, even though Staff's defense of these

requests makes clear that Staff has two particular entities in mind.²⁰

Discovery requests such as Interrogatories 12 and 14 and Document Requests 6 and 8 are precisely the type of inappropriate exertions of agency power that the Federal Trade Commission Improvements Act of 1980 sought to prohibit. *See* S. REP. NO. 96-500 (1979) at 1105 (“The FTC’s broad investigatory powers have been retained but modified to prevent fishing expeditions undertaken merely to satisfy its ‘official curiosity. . . .’”); *see also* Statement of Congressman Shumway, 125 CONG. REC. 32,456 (1979) (noting need to “eliminate” the “propensity for the FTC to engage in ‘fishing expeditions’”); Statement of Congressman Coughlin, 125 CONG. REC. 32,458 (1979) (stating that goal of bill was to “curb this subpoena power by requiring that the Commission specify the conduct they are investigating and why the Commission believes that the conduct violates the law.”). These requests accordingly should be stricken, along with all the other requests in the CID that suffer from the same defect of having been drafted without any effort being made to zero in on a particular activity with respect to which Staff has a genuine concern, based on its investigation to date, of having involved a Section 5 violation.²¹

The inappropriate and unnecessary overbreadth of the CID’s requests is underscored by the fact that WHR has already expended significant time, and incurred out-of-pocket costs in excess of \$ 5 million in drafting written responses to 51 separate questions posed by Staff, preparing oral presentations addressing an additional 29 Staff questions, and locating and producing over 1,010,000 pages of documents in response to 29 separate Staff document requests. *See* Neff Declaration, Exhibit 4, at ¶ 8; Meal Declaration, Exhibit 2, at ¶¶ 5-6 and Exhibit A. Thanks to those extensive efforts on WHR’s part, Staff now has in its possession, for example, over 60 detailed forensic reports regarding the nature and suspected causes of the Intrusions. With that sort of information already in hand, Staff has no reason or need to be fishing about blindly for any and all information and documents that might be out there related to

²⁰ According to Staff, the CID’s broad requests addressing the activities of any and all WHR Service Providers are appropriate because “one of the breaches occurred due to the compromise of a third-party administrative account” and because “the first two breaches involved the intruder accessing files on the Wyndham-branded hotels’ networks . . . [that] were created as a result of the hotels’ property management systems and/or payment processing applications being left in ‘debugging’ mode at the time they were installed on the hotels’ networks by a service provider.” *See* Exhibit 11 hereto, at 2. To begin with, since neither of the entities referenced by Staff in defending these particular requests was actually a WHR Service Provider as defined in the CID (because neither entity was permitted access to personal information, and because the second entity did not even provide services to WHR or its affiliates, *see* Exhibit 1 hereto, Definition V), the entire premise of Staff’s argument is factually incorrect. But even were that not the case, the circumstances described by Staff would hardly begin to justify a wholesale investigation of the activities of each and every one of WHR’s Service Providers. Rather than creating the basis for a fishing expedition of that sort, those circumstances would at most justify a further, targeted Staff inquiry into the activities of the two particular entities that were involved in the circumstances that created the concerns identified by Staff. Thus, far from justifying the CID’s requests addressing the activities of WHR’s Service Providers, Staff’s defense of these requests actually only serves to underscore the fundamental flaws in the CID: Staff’s failure to draft the CID’s requests in a targeted fashion, and Staff’s insistence on instead drafting request after request as broadly as possible in an effort to satisfy Staff’s curiosity about every imaginable aspect of WHR’s information security practices, without giving the slightest regard to whether Staff actually has any reason to believe that the practices being inquired about involved a Section 5 violation.

²¹ The “fishing expedition” category of the CID’s requests includes Interrogatories 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14, and 15, and Document Requests 2, 3, 4, 5, 6, 7, 8, 9, and 10, all of which were drafted without the slightest effort being made to zero in on any particular aspect of WHR’s information security practices that Staff might have some reason to believe to have been involved in a violation of Section 5.

each and every one of WHR's information security practices, including those practices with respect to which there is no reason for Staff to have any concern at all about their having created a risk to consumer data. Instead, what Staff should be doing at this juncture is crafting targeted requests that are drafted to seek with precision whatever limited additional information Staff truly requires at this late date to complete whatever remains of its longstanding investigation. Because the vast majority of the CID's discovery requests were not drafted in this targeted fashion, the CID should be quashed in its entirety or, at a minimum, the non-targeted requests should be stricken. *See D.R. Horton, Inc. v. Leibowitz*, No. 4:10-CV-547-A, 2010 WL 4630210, at *3 (N.D. Tex. Nov. 3, 2010) (noting plaintiff would have strong argument that FTC was "overreaching" when it issued a "CID [that] is so broad that it indicates that no meaningful discretion was exercised by the FTC officials who prepared it").

B. The CID Is Unduly Burdensome

The burden that would be imposed on Wyndham were it required to respond to the requests contained in the CID exactly as they are drafted would be heavy indeed when viewed in isolation, and would be downright absurd when considered in light of the substantial out-of-pocket costs already incurred by WHR in cooperating with the WHR Investigation and the trivial nature of the issues Staff has raised regarding WHR's information security practices after having investigated those practices for a full sixteen months. For this reason as well, the CID should be quashed. *See, e.g., FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977) (a party challenging a subpoena can do so by showing the compliance costs are overly burdensome or unreasonable); *Phoenix Bd. of Realtors, Inc. v. Dep't of Justice*, 521 F. Supp. 828, 832 (D. Ariz. 1981) (the government should negotiate to narrow scope of a CID when compliance may be overly burdensome).

When subparts are counted, the CID's interrogatories contain over 89 distinct questions. When added to the 51 Staff questions WHR has already responded to in writing and the 29 Staff questions WHR has responded to by means of oral presentations, the CID increases the number of questions Staff wants answered as part of the WHR Investigation to a stunning figure of 169—nearly *seven times* more than the 25 interrogatories allowed by both the Federal Rules of Civil Procedure and the Commission's own Rules of Practice for Adjudicative Proceedings. *See* Fed. R. Civ. P. 33(a)(1), 16 C.F.R. § 3.35(a). Moreover, as discussed above, many of the CID's Interrogatories were drafted to cover an extremely broad subject matter and to demand a minute level of detail regarding that subject matter, such that in the case of each of them a substantial fact development and drafting effort would have to be undertaken by inside and outside counsel and Wyndham employees even to begin to provide the requested information.²² For example, Interrogatory 12 seeks, among other things, for each of WWC, WHG, WHR, and WHM, a recitation of every information security test, evaluation, practice, and procedure in existence over a four year time frame, regardless of how informal or trivial the test, evaluation, practice, or procedure. None of these entities keep logs showing each and every step they take with respect to information security—nor could they, since they have numerous employees whose each and every act in their day is geared toward information security. To respond fully to this interrogatory, then, Wyndham would have to review the electronic files of all of these employees

²² See Interrogatories 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, and 21, all of which were drafted in this fashion.

and chronicle every activity each of them undertook during the course of over 1,000 days of work. Based on the sheer number of the CID's interrogatories, and the fact that many of those interrogatories would require an extensive fact development and drafting effort, Wyndham estimates that at least six months of work, and significant out-of-pocket costs would be required to prepare a meaningful response to the CID's interrogatories, and even then the response would be far from complete. See Neff Declaration, Exhibit 4, at ¶ 12. This expenditure (as well as Wyndham's expenditures to respond to the CID's document requests, discussed below,) would of course be *on top of* the \$ 5 million and sixteen months of work that Wyndham has already spent responding to the discovery requests contained in the Access Letter and ensuing Staff communications. See Neff Declaration, Exhibit 4, at ¶ 8.²³

With respect to the CID's document requests, responding to the "all-document requests" included in the CID (Requests 2, 7, 9, 10, 11, 12, 13, 15, 16, and 17) would require a review of the ESI of at least three Wyndham employees, which review would be likely to take about 10 weeks and cost approximately \$1 million. See Neff Declaration, Exhibit 4, at ¶ 11.²⁴ As for the CID's "sufficient to describe requests" (namely, Requests 3, 4, 5, 6, and 14), trying to locate documents "sufficient to describe" the matters addressed in those requests with the breadth, and down to the level of detail, called for by these requests would be hugely burdensome. As reflected in Wyndham's objections to the CID, each of the CID's "sufficient to describe requests" seeks records that are not maintained in the normal course of business in the manner contemplated by the request. See Exhibit 16 hereto, Objections to Document Requests 3, 4, 6, and 7. Thus substantial fact investigation would have to be undertaken as to each such request in order to respond to that request. *Id.* Wyndham estimates that at least six months of work, would be required to prepare a meaningful response to the CID's "sufficient-to-describe" document requests, and even then the response would be far from complete. Adding these numbers to Wyndham's above-described projections for the time and expense that would be required to respond to the other aspects of the CID brings Wyndham's total projection for the time and expense of responding to the CID to at least six months of work²⁵ and an out-of-pocket cost of at

²³ As described in Exhibits 10 and 16, Wyndham also objects to a number of definitions and instructions that it believes impermissibly increase its burden of production. Specifically, Wyndham objects to the CID insofar as it defines terms such as "document", "identify", and "relating to" to have something other than their standard English meanings; insofar as it purports to treat documents as being in Wyndham's possession, custody, and control that would not be treated as such under the Federal Rules of Civil Procedure; insofar as it purports to impose a search obligation on Wyndham beyond the search obligation that would be imposed under the Federal Rules of Civil Procedure; insofar as it imposes protocols for document and information collection and production that are different from those protocols that have been followed by Wyndham thus far in the course of the investigation; insofar as it is addressed to Wyndham Worldwide Corporation rather than to Wyndham; and insofar as it purports to allow only 30 days for compliance.

²⁴ To the extent, as Staff has argued should be the case, the ESI of more than three Wyndham employees were reviewed in order to respond to the CID's all-document requests, the cost of responding to those requests would increase substantially above \$1 million. See Neff Declaration, Exhibit 4, at ¶ 11 .

²⁵ Given the six-month period that Wyndham would require to complete a meaningful (but incomplete) response to the CID, the CID is both unduly burdensome and violative of Section 2.7(b)(1) of the Rules of Practice in purporting to require that Wyndham's complete response to the CID be provided within 30 days of service of the CID. See Exhibit 1 hereto, at 1 (purporting to allow just 30 days for the materials requested by the CID to be provided by Wyndham to Staff); 16 C.F.R. 2.7(b)(1) (providing that civil investigative demands for the production of documentary material shall "provide a reasonable period of time within which the material so demanded may be assembled and made available"). That instruction should therefore be stricken from the CID

least \$2.75 million.²⁶ See Neff Declaration, Exhibit 4, ¶ 12.

Asking Wyndham to invest that amount of time and money in responding to the CID would be utterly indefensible when one considers that this expenditure would be made on top of the 16 months and \$5 million WHR has already spent cooperating with the WHR Investigation, and that Staff's supposed case against WHR based on the WHR Investigation involves just a single alleged Section 5 violation that is marginal at best on the merits and in any event caused no consumer injury. Moreover, there is no reason to think that Wyndham's compliance with the CID would improve the flimsy case Staff believes it has made. For example, WHR has already produced over one million pages of electronic documents²⁷ to Staff from two custodians who were at the heart of dealing with WHR's information security in general and its investigation and remediation of the Intrusions in particular. To date, however, Staff has not once in the course of the WHR Investigation cited to any one of those electronic documents as a basis for arguing that WHR violated Section 5. If the first round of ESI review bore no investigational fruit whatever, why is Wyndham being asked to respond to the CID's all-document requests by going through a second round of ESI review involving a group of less relevant custodians?

Similarly, Wyndham is at a loss to see how the CID's "sufficient-to-describe" document requests or its interrogatories might be expected to buttress the FTC's claim were Wyndham to respond to those discovery requests. The Proposed Complaint contains a single deception-based Section 5 claim, and the key issue in determining the strength of that claim is the interpretation of and the degree of customer reliance on the privacy policy that is the focal point of the claim. Yet none of the CID's interrogatories and "sufficient-to-describe" document requests seek to learn further information about this privacy policy or any customer reliance thereon. Nor is there any likelihood that Wyndham's response to the CID's interrogatories and "sufficient-to-describe" document requests would enable Staff to discover other allegedly deceptive statements by WHR to its customers, given that Staff spent sixteen months trying to do just that but came up with nothing even after WHR fully responded to Staff's question in the Access Letter on the issue of what statements were made to customers regarding the security of their personal information. See Exhibit 3 hereto, Question 13. Staff also has no likelihood of being able to use Wyndham's responses to the CID's sufficient-to-describe document requests and interrogatories to succeed in building at this point an unfairness-based Section 5 claim against WHR of the sort that it was unable to build during the first sixteen months of its investigation, because no matter

²⁶ The burden imposed by the CID is even greater when one considers its demands with respect to privilege. First, the CID requires that Wyndham do the impossible and its claims to privilege with respect to each and every document it intends to withhold as privileged now, before it has had the opportunity to fully investigate the existence of documents responsive to the CID. Exhibit 1, Instruction D. Second, the CID requires that detailed information be provided regarding each document withheld on grounds of privilege. Exhibit 1, Instruction D. Such information can only be logged manually, and the volume of privileged documents is expected to be high in this case due to the extensive involvement of counsel in the events under investigation by the FTC. Third, the CID requires Wyndham to search not just its files but the files of outside counsel, see Exhibit 1, Instruction I. These files are highly likely to be responsive given the breadth of the CID but will almost exclusively be privileged and thus subject to logging requirements. Wyndham objects to both of these instructions and does not waive any rights to withhold documents as privileged.

²⁷ The phrase "electronic documents" refers to documents produced from custodial files with full electronically stored information under the Bates prefix WHR-FTC2, as opposed to the documents produced under the Bates label WHR-FTC1, which are paper or other documents produced to respond to specific Staff requests.

what evidence Staff might adduce through the CID of security vulnerabilities at WHR or the Wyndham-branded hotels, Staff still would have no way of demonstrating the substantial consumer injury that would be the linchpin of any such claim. In short, the huge cost Wyndham would incur in responding to the CID is completely disproportionate to any investigatory value the CID could possibly have to the WHR Investigation.

The CID is also unduly burdensome in that it repeats, in whole or in part, numerous discovery requests to which WHR has already responded during the course of the WHR Investigation. Specifically, Wyndham's review of the Access Letter and the additional Staff questions answered by WHR during the course of the WHR Investigation reveals that WHR has already been asked, in whole or in part, at least 42 of the CID's 89 interrogatories and at least 25 of the CID's 38s document requests. *See* Meal Declaration, Exhibit 2, at ¶¶ 8-9 and Exhibits C and D. In some cases, the CID even restates the prior question almost verbatim. Compare Access Letter (Exhibit 13 hereto), Question 6 (a)-(d), with CID (Exhibit 1 hereto), Interrogatory 4 (a)-(d); and compare Access Letter (Exhibit 3 hereto), Question 13, with CID (Exhibit 1 hereto), Interrogatory 21 and Document Request 15.²⁸ Staff purports to defend its failure to draft the CID so as to be non-duplicative of Staff's prior discovery requests by inviting *Wyndham* to undertake the effort first to re-review all Staff's prior discovery requests and then to re-write the CID to eliminate its many duplicative aspects. *See* CID (Exhibit 1 hereto), at Instruction K; Exhibit 11 hereto at 3 (Staff letter suggesting that Wyndham "can comply with the CID by referencing its previous submissions" when Wyndham responds to the CID's duplicative requests). This approach to curing Staff's failure to draft the CID by taking due care not to unduly burden Wyndham would require *Wyndham* to expend the significant time and effort that would be required to fix Staff's drafting error. Forcing a CID recipient to go to such lengths would fly in the face of the legislative scheme that governs the issuance of FTC CIDs. *See* Statement of Senator Heflin, 125 CONG. REC. 2394-96 (1980) (criticizing FTC for forcing company to spend \$200,000 merely to evaluate burden of complying with subpoena and noting that Federal Trade Commission Improvements Act of 1980 was intended to restrict such behavior). Thus, instead, of making Wyndham bear the burden of correcting Staff's drafting deficiencies, the appropriate cure for Staff's failure to lift a finger to craft the CID's requests so that they seek only new information is for each and every discovery request in the CID to be stricken in its entirety to the extent it in whole or in part duplicates one of Staff's prior requests in the course of the WHR Investigation.²⁹

C. The CID Is Too Indefinite in Numerous Respects

"Indefiniteness" is one of the recognized bases for quashing a CID. *U.S. v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (citing indefiniteness as one of three bases for quashing CID); *see SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512, 514 (10th Cir. 1980) (citing *Morton Salt*, 338

²⁸ Despite this, Staff has obstinately refused to acknowledge the repetitiveness of the CID's requests. *See* Exhibit 11 hereto at 2-3 (Staff letter stating that "we do not believe the CID contains any requests that were previously answered by Wyndham in response to the access letter").

²⁹ Under this approach, Interrogatories 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, and 21, and Document Requests 2-7 and 9-17 (all of which in substantial part duplicate discovery requests Staff has previously made and WHR has already fully responded to), *see* Meal Declaration (Exhibit 2 hereto), at ¶¶ 10-11 and Exhibits C-D would be stricken in their entirety.

U.S.) (confirming that “[t]o obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met”). A CID is deemed “too indefinite” when it fails to “describe each class of material to be produced with such definiteness and certainty as to permit such material to be fairly identified.” 11 C.F.R. 2.7(b)(1); Operating Manual, § 3.3.6.7.5.3(1). Here, as described below, many of the CID’s requests were drafted without any attention having been given to the generality of the request, the level of detail demanded by the request, or the lack of clarity of the request. Because those requests therefore were not drafted so as to permit the requested material to be “fairly identified” by Wyndham, each of those requests should be stricken.

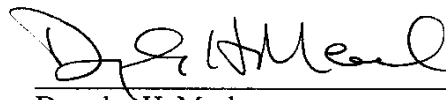
To begin with, many of the requests in the CID manage to seek information or documents both at a very high level of generality and, at the same time, at an extreme level of detail. For example, Interrogatory 3 seeks information as to “how the Wyndham-branded hotels’ networks are connected to any Company network(s)” — a broad question, particularly given that “connected” is not defined to be limited to be via computer or internet. The request appears to encompass both a listing of databases and systems on the computer networks of the Wyndham entities that can be accessed from the Wyndham-branded hotels and the specific technology used to make these connections. The Interrogatory then asks for a number of pieces of information, several of which go beyond the question of how the networks are connected to inquiring about security of information in certain databases and systems: “whether and how the Wyndham-branded hotels may access the central reservation system(s) or guest loyalty database(s),” “the personal information contained in each”, “any access controls in place to limit access to the central reservation system or guest loyalty database.” Interrogatory 3, therefore, asks Wyndham to narrate for Staff any and all knowledge it has regarding connections between any Wyndham entity and the Wyndham-branded hotels, without focusing on any specific system or database or other means of connection relevant to this case. A request like that does not come close to describing the information or documents being requested with “with such definiteness and certainty as to permit such material to be fairly identified.” Interrogatory 3 therefore must be stricken as being “too indefinite,” as must Interrogatories 2, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, and 21, and Document Requests 2-7 and 9-17, all of which suffer from this same sort of indefiniteness as to exactly what information or documents the request in question is asking to be provided.³⁰

CONCLUSION

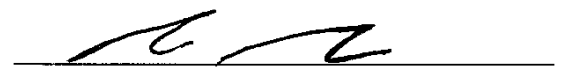
For all of the foregoing reasons, as well as those set forth in the accompanying Exhibits, Wyndham respectfully requests that the Commission quash or, alternatively, limit the CID as set forth above.

³⁰ The CID is also “too indefinite” by reason of the lack of definiteness and clarity created by the CID’s use of definitions that vary the standard English meaning of terms like “document”, “identify”, and “relating to” to have something other than their standard English meanings. See CID (Exhibit 1 hereto), Definitions J, O, and U. These definitions therefore should likewise be stricken.

Dated: January 20, 2012



Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517 (Telephone)
(617) 235-0232 (Facsimile)
douglas.meal@ropesgray.com



Seth C. Silber
WILSON, SONSINI, GOODRICH & ROSATI
1700 K Street, NW, Fifth Floor
Washington, DC 20006
(202) 973-8800 (Telephone)
(202) 973-8899 (Facsimile)
ssilber@wsgr.com

*Attorneys for Petitioners Wyndham Hotels &
Resorts, LLC and Wyndham Worldwide
Corporation*

CERTIFICATE OF SERVICE

I hereby certify that, on January 20, 2012, I caused the original, twelve (12) copies, and a compact disc of Wyndham Worldwide Corporation and Wyndham Hotels & Resorts, LLC's Petition to Quash or, Alternatively, Limit Civil Investigative Demand with attached exhibits to be hand delivered to the Secretary of the Federal Trade Commission at the following address:

Federal Trade Commission
600 Pennsylvania Ave., NW
Room H-159
Washington, D.C. 20580

A handwritten signature in blue ink, appearing to read "David T. Cohen", written over a horizontal line.

David T. Cohen



United States of America
Federal Trade Commission

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

<p>4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN</p> <p>Kristin Krause Cohen 601 New Jersey Ave., NW NJ-8100 Washington, DC 20001 Deputy Records Custodian: Lisa Schifferle</p>	<p>5. COMMISSION COUNSEL</p> <p>Kristin Krause Cohen/Lisa Schifferle 601 New Jersey Ave., NW NJ-8100 Washington, DC 20001 (202) 326-2276/(202) 326-3377</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------

DATE ISSUED 12/8/11	COMMISSIONER'S SIGNATURE <i>Julie Brill</i>
------------------------	------------------------------------------------

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, *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

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

A handwritten signature in blue ink, appearing to read "D. H. Meal", written over a horizontal line.

Douglas H. Meal

**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

**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.

**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

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

No.	Interrogatory	Prior Request
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



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

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

Lisa W. Schifferle
Attorney
Division of Privacy & Identity Protection

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.

CONFIDENTIAL

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

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

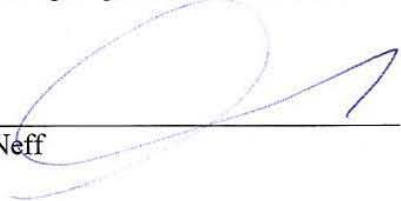
10. Though the CID is significantly duplicative of the requests made by the FTC in the access letter and subsequent communications, Wyndham estimates that compliance with the “all-document requests” contained in the CID would require a full review of the electronic files of three additional custodians.

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

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,)
)

DOCKET NO. C-

WYNDHAM HOTELS & RESORTS, LLC,)
a limited liability company,)
)

and)
)
)

WYNDHAM HOTEL MANAGEMENT, INC,)
a corporation.)
_____)

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.

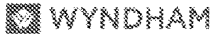
- (b) In May 2009, respondents learned that intruders had again installed memory-scraping malware on Wyndham Hotels' network and on the networks of twenty Wyndham-branded hotels. In addition, the intruders re-configured some of the Wyndham-branded hotels' software so that new payment card information 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 -

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

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

In the Matter of)	
)	
WYNDHAM WORLDWIDE CORPORATION,)	FILE NO: 1023142
a corporation,)	
)	
WYNDHAM HOTEL GROUP, LLC,)	AGREEMENT CONTAINING
a limited liability company,)	CONSENT ORDER
)	
WYNDHAM HOTELS & RESORTS, LLC,)	
a limited liability company,)	
)	
and)	
)	
WYNDHAM HOTEL MANAGEMENT, INC,)	
a corporation.)	
)	

The Federal Trade Commission has conducted an investigation of certain acts and practices of Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LLC, and Wyndham Hotel Management, Inc. (collectively “proposed respondents”). Proposed respondents, having been represented by counsel, are willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LLC, and Wyndham Hotel Management, Inc. by their duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent Wyndham Worldwide Corporation is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054.
2. Proposed respondent Wyndham Hotel Group, LLC is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany,

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

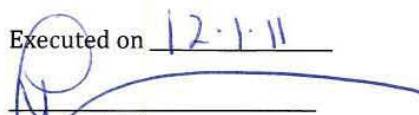
CERTIFICATION DECLARATION

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

	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

STATEMENT PURSUANT TO 16 C.F.R. § 2.7(d)(2)

Pursuant to 16 C.F.R. § 2.7(d)(2), counsel for Wyndham Hotels and Resorts, LLC and its parent company, Wyndham Worldwide Corporation (together, “Wyndham”) hereby state that they conferred with counsel for the Commission in an effort in good faith to resolve by agreement the issues raised by this Petition to Quash, but have been unable to reach such an agreement. A teleconference between Wyndham and Commission counsel occurred on January 6, 2012, starting at 1:30 p.m. Douglas Meal and Rachel Rubenson of Ropes & Gray LLP and Lydia Parnes and Seth Silber of Wilson Sonsini Goodrich & Rosati participated in the teleconference for Wyndham, while Kristin Cohen, Lisa Schifferle, and Kevin Moriarty participated for the Commission. Subsequently, counsel for Wyndham and counsel for the Commission exchanged letters, which are attached as Exhibits to this Petition. While Commission counsel agreed in a January 12, 2012 letter to recommend one modification to the Associate Director relating to one of the CID’s definitions, Wyndham did not receive any confirming correspondence from the Associate Director, and has otherwise been unable to come to an agreement with Commission counsel on the issues presented by this Petition.

A handwritten signature in blue ink, appearing to read "Douglas H. Meal", is written over a horizontal line.

Douglas H. Meal



ROPES & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPESGRAY.COM

January 8, 2012

Douglas H. Meal
T +1 617 951 7517
F +1 617 235 0232
douglas.meal@ropesgray.com

BY EMAIL

Kristin Krause Cohen, Esq.
Division of Consumer Privacy and Protection
Bureau of Consumer Protection
601 New Jersey Avenue NW
Washington, DC 20580

Re: Wyndham Hotels and Resorts – Confidential Submission to Federal Trade Commission

Dear Kristin:

Thank you for your letter dated January 6, 2012. We are confused by the request contained in your letter. During our teleconference, we in fact did put forth a “specific proposal” on behalf of Wyndham Hotels & Resorts LLC (“Wyndham”) relative to how the Commission’s December 8, 2011 Civil Investigative Demand (“CID”) might be modified so as to enable Wyndham and the Commission’s staff (“Staff”) to resolve Wyndham’s objections to the CID’s invalidity, overbreadth, and burdensomeness. Since you evidently did not understand us to have made such a proposal, we will recapitulate it here.

Our proposal is premised on the fact that, ostensibly, the CID is intended to enable Staff to obtain whatever limited additional discovery it still needs from Wyndham in order to complete its now nearly two-year-old investigation into whether Wyndham’s information security practices comply with Section 5 of the Federal Trade Commission Act. As we pointed out in our teleconference, Wyndham does not believe Staff in fact has any such need for additional discovery from Wyndham. Staff has previously advised Wyndham that, based on Staff’s investigation to date, Staff is prepared to recommend corrective action to the Commission in the form of a consent agreement. Indeed, Staff has already provided Wyndham with the consent agreement it is prepared to recommend to the Commission and a proposed Complaint alleging violations of Section 5 on the part of Wyndham and certain of its affiliates. Obviously, then, Staff has already determined that its investigation has adduced sufficient information from which the Commission may conclude that it has reason to believe that Wyndham’s information security practices violate Section 5. Any investigation that has reached a point at which Staff has made such a determination and is ready to make such a recommendation is by definition “complete,” because once an investigation reaches that point Staff by definition has no need for any further information in order to conclude the investigatory phase of

the case (see FTC Operating Manual Section 1.3.4.4) and proceed with the next phase of the case (see FTC Operating Manual Chapters 3 & 6). At this juncture, then, any further discovery Staff might seek from Wyndham would not truly be for the purpose of investigating whether there is reason to believe that Wyndham violated Section 5 (as the Staff has already determined that to be the case), but instead would in fact be for the purpose of aiding Staff's anticipated effort to prevail in litigation against Wyndham once its Complaint is filed. However, discovery of *that* sort is supposed to be sought and obtained by Staff not in the guise of completing an already-completed investigation, but rather under and subject to the Commission's rules for adjudicative proceedings, and only to the extent such discovery is authorized by the presiding ALJ.

Moreover, even assuming Staff has a genuine need for yet additional discovery from Wyndham in order to complete this long-standing investigation, such discovery should at this juncture be quite limited in nature. As you are aware, Wyndham has already voluntarily provided Staff with massive amounts of information in the course of this investigation, and has incurred substantial expense in so doing. In particular, Wyndham has already produced to Staff over one million pages of documents in response to the document requests in the Commission's April 10 access letter and ensuing Staff communications; Wyndham has already submitted to Staff four separate detailed written narratives responding to the questions posed in those communications; and Wyndham's Chief Information Security Officer and/or inside and outside counsel have already made nine separate in-person presentations to Staff in an effort to address various questions Staff has raised. That being the case, Staff should at this point have very few remaining requests for yet additional information from Wyndham, and any such remaining requests should be of the "rifle-shot" variety, i.e., they should be capable of being drafted to target precisely the particular pieces of additional information Staff is looking for, with care being taken not to duplicate Staff's previous requests and not to impose significant burden on Wyndham in responding to those additional requests.

Unfortunately, the CID was not drafted in anything remotely resembling this fashion. To the contrary, it is a classic "kitchen-sink" discovery request that takes no account whatever of Staff's previous requests and Wyndham's previous responses to those requests, and makes no effort whatever to avoid unduly burdening Wyndham in responding to the CID. Including sub-parts, the CID includes no fewer than *eighty-nine* separate interrogatories and *thirty-six* separate document requests. As drafted, Wyndham would be required to expend months if not years of time, not to mention millions of dollars, even to begin to respond to the CID's interrogatories and document requests, and even then most of the CID's discovery requests would prove impossible to respond to fully. By way of example only, Interrogatory 12 purports to require Wyndham to describe in detail each and every aspect of any and all information security measures that Wyndham had in place at any time during the last four years, including the date on which each and every such aspect was implemented, each and every assessment, test, evaluation, monitoring action, or change that was made of or to any such aspect during such period, and the date of every such assessment, test, monitoring action, or change. No account is given in this interrogatory to the voluminous amount

of information that Staff has already received from Wyndham in regard to its information security during the period in question. No effort is made in this interrogatory to zero in on any particular aspect of Wyndham's information security that Staff might have concerns about based on its investigation to date. No attention is paid in this interrogatory to the obvious fact that any company's information security measures are routinely being assessed, tested, evaluated, monitored, and changed not just daily but minute-by-minute, such that the net effect of this interrogatory as drafted is to ask that Wyndham undertake an effort to somehow create for Staff a comprehensive daily history of every detail of every aspect of every feature of Wyndham's information security over a four-year period.

Nearly all of the CID's interrogatories and document requests suffer from the twin defects of both duplicating discovery requests Staff has previously made and being drafted without any attention having been given to the generality of the request, the level of detail demanded by the request, and/or the information Wyndham has already provided within the ambit of the request. See, for example, Interrogatories 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, and 21, and Document Requests 2-7 and 9-17. Moreover, many of the CID's interrogatories and document requests address in whole or in part areas, such as the information security practices of Wyndham's service providers (Interrogatory 14 and Document Request 8) and affiliates (see Interrogatories 5, 6, 7, 8, 12, 13, 14, 16, 17, 18, 19, 20, and 21, and Document Requests 3, 6, 7, 8, 9, 10, 12, 13, and 16), that have not been part of Staff's investigation up to this point¹ and as to which Staff has no basis now to expand its investigation.

¹ During our teleconference, you stated that you believed Staff's investigation has from its inception extended to Wyndham's affiliates and their information security practices. You are incorrect. The Commission's access letter dated April 8, 2010 was addressed solely to Wyndham Hotels and Resorts LLC and expressly states in its very first sentence that Staff was conducting "a non-public investigation into Wyndham Hotels and Resorts LLC's ("Wyndham") compliance with federal laws governing information security." The second sentence of the letter then states that "[w]e seek to determine whether *Wyndham's* information security practices comply with Section 5 of the Federal Trade Commission Act" (emphasis supplied). While the access letter later incoherently purported to redefine the term "Wyndham" to include Wyndham's affiliates and a number of other entities for purposes determining the scope of the access letter's discovery requests, that redefinition did not alter the letter's earlier clear statement that the sole entity actually under investigation by the Commission was Wyndham Hotels and Resorts LLC and the only information security practices being investigated were those of Wyndham Hotels and Resorts LLC. Moreover, we are aware of no subsequent communication from the Commission to any Wyndham affiliate advising such affiliate that it too was a target of this investigation or any other investigation being conducted by the Commission.

Nothing that has transpired in the investigation to date could possibly be thought to justify the enormous discovery burden that the CID would impose on Wyndham. To the contrary, the results of the investigation only serve to underscore the CID's gross impropriety. To begin with, as you are well aware, because payment card data was the only personal information placed at risk of compromise during the events in question, and because payment card issuers protect their cardholders against suffering any financial injury by reason of their payment card data being compromised, *the investigation has not revealed even a shred of evidence of any consumer injury having occurred as a result of Wyndham's information security practices.* Indeed, the absence of substantial consumer injury is so clear in this case that Staff's proposed Complaint does not even bother to include an unfairness-based Section 5 claim against Wyndham. Rather, the proposed Complaint is limited to a deception-based Section 5 claim. But even that claim presents insignificant consumer protection concerns, for the claim is based entirely on a privacy policy that there is no reason to believe was even read, much less relied upon in making a purchasing decision, by any appreciable number of Wyndham customers (if, indeed, by any at all), and the validity of the claim depends entirely on Staff's tortured reading of a single sentence in that multi-paragraph policy – a reading that is elsewhere expressly negated by the policy itself.

In view of the CID's pervasive duplication of Staff's prior requests, its patent overbreadth in seeking to expand the investigation at the eleventh hour to Wyndham's affiliates and service providers, and its unjustifiable burdensomeness when one takes into account the vast amount of information Wyndham has already provided to Staff and trivial nature of the Section 5 violation that Staff believes it has found, it is obvious to us, and we believe it would be obvious to a court even if it were not obvious to the Commission, that the CID in no way, shape, or form represents a good faith attempt by Staff to request of Wyndham merely whatever minimal additional discovery Staff might at this juncture legitimately believe it needs to complete this investigation. To the contrary, we believe a court would find that the CID was drafted and served for the improper purpose of coercing Wyndham into accepting the Staff settlement terms being objected to by Wyndham – settlement terms that, as demonstrated in the whitepaper delivered by Wyndham to Staff on November 21, 2011, Staff has no basis in fact or law for seeking to impose on Wyndham. In this regard, we expect that a court would find it no mere coincidence that the CID just happened to be served within a few weeks after Wyndham's whitepaper was delivered, and we think a court would find it telling that even now, nearly seven weeks after the whitepaper was delivered, Staff has provided Wyndham with no rebuttal of any sort to the arguments Wyndham advanced in the whitepaper as to the unlawfulness of the settlement terms being demanded by Staff.

For the reasons set forth above, among others (including the invalidity of the CID due to its failure to be predicated on a proper investigatory resolution on the part of the Commission or on a proper showing of need on the part of the Staff), Wyndham is confident that the CID would be quashed in its entirety by a court if it were not quashed by the Commission itself. Wyndham therefore has no intention of responding to the CID as drafted. Having said that, as we stated during our January 6

teleconference, Wyndham is prepared to resolve its objections to the CID's invalidity, overbreadth, and burdensomeness by the Staff's agreeing to revise the CID so that it is limited to seeking a reasonable amount of additional discovery that could legitimately be considered necessary to the completion of Staff's investigation and that would not unduly burden Wyndham. To that end, during our teleconference we proposed that Staff revise the CID as follows:

Generally, we proposed that Staff redraft the interrogatories and document requests so as to eliminate those portions that (1) relate to any Wyndham service provider's or affiliate's information security practices (there being no basis for Staff at this late juncture to expand its investigation into such security practices) or (2) duplicate a prior interrogatory or document request interposed by Staff (there being no basis for Staff to engage in such duplicative discovery). In this latter regard, we disagreed with your suggestion that it is Wyndham's duty, and not Staff's, to revise the CID's discovery requests to cure the patently duplicative aspect of the vast majority of those requests.²

In regard to the interrogatories, in addition to redrafting the interrogatories in accordance with our general proposals described above, we proposed that Staff reduce the number of interrogatories from 89 to no more than 10 including subparts (there being no basis for Staff at this late juncture of its investigation to interpose such a substantial number of interrogatories) and that each interrogatory be drafted so as to seek with precision particular information that Staff has not previously requested, that reasonably relates to the subject matter of the investigation, and that would reasonably be expected to be readily accessible to Wyndham (there being no basis for Staff at this juncture to interpose interrogatories that would impose on Wyndham the enormous burden of

² While our teleconference did not address our further general objections to the CID's discovery requests, we note here that we also generally object to the CID insofar as it defines "personal information" to include information other than the type that was allegedly placed at risk of compromise during the intrusions and/or information that is beyond the FTC's statutory jurisdiction (such as "employees" information); insofar as it seeks documents protected by the attorney-client, work product, or other privilege; insofar as it requires a privilege log (at least one as detailed as set forth in the CID); insofar as it defines terms such as "document", "identify", and "relating to" to have something other than their standard English meanings; insofar as it purports to treat documents as being in Wyndham's possession, custody, and control that would not be treated as such under the Federal Rules of Civil Procedure; insofar as it purports to impose a search obligation on Wyndham beyond the search obligation that would be imposed under the Federal Rules of Civil Procedure; insofar as it imposes protocols for document and information collection and production that are different from those protocols that have been followed by Wyndham thus far in the course of the investigation; insofar as it is addressed to Wyndham Worldwide Corporation rather than to Wyndham; insofar as it purports to allow only 30 days for compliance; and insofar as it treats the relevant time period as extending beyond May 2010. Our proposal should accordingly be read to include a request that these aspects of the CID be redrafted as well.

the months of painstaking research that would be required even to try to answer Interrogatories 2-10, 12-15, 18-20, and 23-25 as written, especially given that Wyndham has already provided Staff with extensive amounts of information responsive to many of those interrogatories). In this regard, we disagreed with your suggestion that it is Wyndham's duty, and not Staff's, to revise Staff's interrogatories to cure the extreme burdensomeness of the vast majority of those interrogatories as drafted by Staff, though we did provide you with a couple of examples of interrogatories that we considered to have been properly drafted.

In regard to the document requests, in addition to redrafting the document requests in accordance with our general proposals described above, and in addition to reducing the overall number of requests to no more than 10 including subparts, we proposed that any "all documents" requests (namely, requests such as Requests 2, 7, 9, 10, 11, 12, 13, 15, 16, and 17) be handled by Staff's designating up to three additional custodians (we suggested Copenheaver, Armstrong, and Burger) whose documents would be reviewed in an effort to locate documents responsive to those requests. We further proposed that the "sufficient to describe" requests (namely, Requests 3, 4, 5, 6, and 14) be withdrawn entirely, owing to the extreme burden associated with trying to locate documents "sufficient to describe" the matters addressed in those requests with the breadth, and down to the level of detail, called for by these requests, and owing to the fact that Wyndham has already provided Staff with substantial information regarding those matters (such as the detailed presentation Wyndham made in December 2011 on the subject matter of Request 14—which subject matter, incidentally, has nothing whatever to do with Staff's investigation). In place of the sufficient to describe requests, and subject to the overall 10-request limit, we proposed that Staff draft new requests that seek with precision particular documents that Staff has not previously requested, that reasonably relate to the subject matter of the investigation, and that would reasonably be expected to be readily accessible to Wyndham.

We trust the above clarifies the specific proposal we made on behalf of Wyndham on January 6. We look forward to hearing Staff's response to that proposal.

Very truly yours,



Douglas H. Meal

cc: Lydia Parnes
cc: Lisa Schifferle



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

Kristin Krause Cohen
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection

Direct Dial: 202.326.2276
Fax: 202.326.3629
Email: kcohen@ftc.gov

January 12, 2012

BY E-MAIL

Lydia Parnes
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW
Washington, DC 20006

Douglas H. Meal
Ropes & Gray, LLP
One International Place
Boston, MA 02110

Dear Doug and Lydia:

We write in response to your January 8, 2012 letter regarding the Federal Trade Commission's ("FTC") Civil Investigative Demand ("CID") to Wyndham Worldwide Corporation ("Wyndham"). As I stated in our January 6, 2012 telephone conference, the FTC has a legitimate need for each item of information requested in the CID. That said, the FTC is willing to make reasonable modifications to the CID in ways that will satisfy the needs of our investigation and address, when possible, the concerns of your client as expressed in your letter.

First, Wyndham appears to object to anything more than a "rifle-shot" request for information because, as you argue, "by definition" the FTC's investigation must be complete. This misconstrues the procedural posture of this matter. At Wyndham's request, the FTC suspended its investigation in order to explore settlement, and the proposed consent agreement arose out of those negotiations. You incorrectly suggest that these events signaled the completion of the investigation. Indeed, the FTC has repeatedly informed Wyndham that if a settlement was not reached, we would resume our investigation. Your suggestion that the FTC is acting in bad faith is troubling, and contrary to the spirit of compromise with which the FTC acceded to your request to suspend the investigation while the parties entered settlement negotiations.

As we stated in our letter of January 6, we are unable to modify the CID absent specific proposals for modification beyond mere general objections to duplication and overbreadth and an arbitrary cap on the number of interrogatories. Where we were able to construe a specific

PUBLIC

request for modification of the CID from your January 8 letter, we address it below, and we remain open to a more specific dialog regarding your outstanding concerns.

Affiliates: You challenge the application of the CID to entities other than Wyndham Hotels and Resorts LLC (“WHR”), and have requested that the CID be modified to eliminate any specifications seeking information related to the information security practices of any WHR affiliate. Among other things, this CID requests information related to Wyndham Hotel Group (“WHG”), Wyndham Worldwide Corporation (“WWC”), and Wyndham Hotel Management (“WHM”) – information that by counsel’s own admission, Wyndham did not provide in response to the FTC’s access letter. In your access letter responses, you explained that WHR’s information security program was handled first (during the time of the first two breaches) by WHG, and thereafter (at the time of the third breach) by WWC. Moreover, Wyndham’s access letter responses also made clear that several of the hotels breached were managed by WHM, and that WHM was responsible for the information security at those hotels. Accordingly, the CID specifications seeking information on the roles each of these Wyndham entities played in the information security of WHR, WHM, and the Wyndham-branded hotels are entirely appropriate.¹ We will consider, however, any reasonable requests to modify any particular specification as it relates to a particular Wyndham entity that you would like to propose.

Service Providers: You also have objected to any CID specifications referencing Wyndham service providers. This information is highly relevant to our investigation since your access letter response explained that one of the breaches occurred due to the compromise of a third-party administrative account. Moreover, as you know, the first two breaches involved the intruder accessing files on the Wyndham-branded hotels’ networks containing clear text payment card information. These files were created as a result of the hotels’ property management systems and/or payment processing applications being left in “debugging” mode at the time they were installed on the hotels’ networks by a service provider. Therefore, Wyndham’s role in the oversight of both its own service providers, as well as the Wyndham-branded hotels’ service providers, is both appropriate and necessary.

Specifications Seeking “All Documents”: You have suggested that the interrogatories requesting “all documents” should be limited to particular custodians. We agree that this is a reasonable suggestion. We do not believe, however, that it is possible to identify the same three custodians for every interrogatory. Instead, the custodians searched should vary based on the subject of the interrogatory and which custodian is likely to have responsive information. Please contact us as soon as possible to discuss appropriate custodians.

Duplicative Requests. You have requested that we modify the CID to eliminate any portions that duplicate a prior interrogatory or document request interposed by Staff. You have not laid out with specificity what is duplicative about any of the CID’s specifications, and we do not believe the CID contains any requests that were previously answered by Wyndham in

¹ Moreover, we also believe it is appropriate to address the CID to WWC, given that the other Wyndham entities whose practices are at issue are its wholly-owned subsidiaries, and it currently controls their data security practices.

response to the access letter. As you know, pursuant to Instruction K, if Wyndham has previously produced any documents responsive to this CID, or previously answered any interrogatories, it can comply with the CID by referencing its previous submissions. If Wyndham would like to raise with us any specific specification that it believes is duplicative, we would be happy to discuss it further.

Personal Information Definition: You have objected to the definition of personal information as including information other than the information compromised as a result of the breaches (namely payment card information), and have specifically requested that employee information be excluded from the definition. We will recommend to our Associate Director that the CID be modified to include in the definition of personal information only customer information.

Privilege Log: You have objected to the CID's requirement that Wyndham provide a privilege log for any material responsive to the CID that is withheld on the basis of a claim of privilege. We believe a privilege log is necessary, but will consider any modifications to the specific requirements of Instruction D to the CID that achieves our objective while addressing Wyndham's concerns.

30-Day Response Deadline: You have objected to the CID's return date giving Wyndham 30 days in which to comply. As you know, at your request, on December 15, 2011, we modified the deadlines in the CID for the meet and confer (from December 22, 2011 to January 6, 2012) and for production (from January 9, 2012 to January 30, 2012). Accordingly, Wyndham was actually given a response deadline of 51 days. Nevertheless, Wyndham waited until January 6 to raise any objections to the CID, and until January 8 to object to meeting the CID's already-extended deadline. That said, we will consider any reasonable request Wyndham makes to extend the production deadline, so long as the request meets the FTC's legitimate need to receive the information requested in a timely manner.

Other Requests: You have raised other general concerns regarding the CID, including objecting to 1) all document requests seeking "documents sufficient to describe"; 2) the definitions of "document"; "identify"; and "relating to" in so far as the definitions differ from "standard English meanings"; 3) the CID's instruction on Wyndham's search obligation; 4) the applicable time period for the CID; and 5) any CID instruction requiring Wyndham to produce information using a protocol different than that used in its response to the access letter. We believe these objections as a whole are unfounded. As to each of these issues, however, we remain open to discussing with you any legitimate concerns you may have. For example, if Wyndham would like to discuss limiting the applicable time period for any particular CID specification, we are open to considering such a request.

With regards to Wyndham's other concerns, as we stated in our call and again in our letter of January 6, it is impossible for us to respond further to your concerns if you are unwilling or unable to identify why you believe specific interrogatories and requests are inappropriate. For example, you state that you will not respond to Interrogatories 2-10, 12-15, 18-20, and 23-25 because both (a) you already have responded by providing "extensive" information, and (b) responding would require "months of painstaking research." (Letter at 5-6.) It is difficult for us

to understand how a question can be, at the same time, impossible to answer and already answered. In order to consider any CID modifications, we need specific proposals beyond simply general objections related to purported duplication and overbreadth.

We look forward to the timely resolution of any remaining issues regarding the CID. To that end, please provide us with any additional, specific concerns with the CID as soon as possible.

Best Regards,

A handwritten signature in black ink, appearing to read 'Krause', written in a cursive style.

Kristin Krause Cohen
Attorney
Division of Privacy and Identity Protection



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

Kristin Krause Cohen
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection

Direct Dial: 202.326.2276
Fax: 202.326.3629
Email: kcohen@ftc.gov

January 6, 2012

BY E-MAIL

Lydia Parnes
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW
Washington, DC 20006

Douglas H. Meal
Ropes & Gray, LLP
One International Place
Boston, MA 02110

Dear Doug and Lydia,

This letter follows our teleconference of earlier today regarding Wyndham Worldwide Corporation's ("Wyndham") responses to the Commission's December 8, 2011 Civil Investigative Demand ("CID") in our investigation related to unauthorized access to the computer network of Wyndham Hotels and Resorts, LLC, along with the networks of several of its franchisees and hotels managed by Wyndham's subsidiary, Wyndham Hotel Management, Inc.

During our discussion today you indicated that you believe that responding to the CID as propounded would be burdensome for your clients. As we stated during our call, we do not believe the scope of the CID as propounded is burdensome. As we indicated, however, we are happy to seriously consider any reasonable requests for modification to the CID that you propose. This Division is committed to reaching good faith agreements with Wyndham that will allow your clients to respond efficiently and timely to the Commission's CID. In order to consider such a request for modification to the CID, and as we discussed, we need you to provide specific proposals.

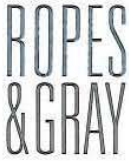
PUBLIC

We look forward to receiving your specific proposals as soon as possible, but in any event by Wednesday, January 11, 2012. In the interim, you are welcome to contact me at (202) 326-2276.

Best Regards,

Handwritten signature of Kristin Krause Cohen in black ink, including the initials "KKH" at the end.

Kristin Krause Cohen
Attorney
Division of Privacy and Identity Protection



ROPES & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPESGRAY.COM

January 13, 2012

Douglas H. Meal
T +1 617 951 7517
F +1 617 235 0232
douglas.meal@ropesgray.com

BY EMAIL

Kristin Krause Cohen, Esq.
Division of Consumer Privacy and Protection
Bureau of Consumer Protection
601 New Jersey Avenue NW
Washington, DC 20580

Re: In the Matter of Wyndham Hotels and Resorts –Federal Trade Commission File No.: 1023142

Dear Kristin:

Please refer to the Commission's December 8, 2011 Civil Investigative Demand ("CID") in the above-referenced matter. Capitalized terms not otherwise defined herein have the meanings ascribed to such terms in the CID.

In connection with the Petition to Quash the CID that Wyndham Hotels & Resorts LLC ("WHR") and Wyndham Worldwide Corporation ("WWC") anticipate filing with respect to the CID, please provide the following documents to the undersigned at your earliest convenience and in any event by no later than the close of business on January 18, 2012:

1. The memorandum submitted to the Commission pursuant to Section 3.3.6.7.3 of the Commission's Operating Manual, requesting approval of the purported investigational resolution attached to the CID.
2. The memorandum submitted to the Commission pursuant to Section 3.3.6.7.5.4 of the Commission's Operating Manual, requesting issuance of the CID.
3. The memorandum submitted to the Commission or the Director of the Bureau of Consumer Protection pursuant to Section 3.3.5.1.2 of the Commission's Operating Manual, requesting approval of the investigation described in the first paragraph of the Access Letter (the "Investigation"), together with the documentation by which the Commission or the Bureau Director approved such request.

ROPES & GRAY LLP

Kristin Krause Cohen, Esq.

- 2 -

January 13, 2012

4. Any memorandum or other document submitted to the Commission or the Director of the Bureau of Consumer Protection pursuant to Section 3.3.5.1.2 of the Commission's Operating Manual or otherwise requesting approval that the Investigation (or any other investigation being conducted by the Commission's staff) include WWC or any of WHR's other affiliates as proposed respondents and/or extend to the information security practices of WWC, any of WHR's other affiliates, or any of WHR's service providers, together with the documentation by which the Commission or the Bureau Director approved any such request.

5. Any documentation by which WWC or any of WHR's other affiliates was, according to the Commission, given notice pursuant to Section 3.3.6.1 or otherwise that it was a proposed respondent in the Investigation or any other investigation being conducted by the Commission's staff.

Thank you for your prompt attention to these requests. Please contact me if you have any questions.

Very truly yours,

Handwritten signature of Douglas H. Meal in blue ink.

Douglas H. Meal

cc: Lisa Schifferle



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

Kristin Krause Cohen
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection

Direct Dial: 202.326.2276
Fax: 202.326.3629
Email: kcohen@ftc.gov

January 17, 2012

BY E-MAIL

Lydia Parnes
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW
Washington, DC 20006

Douglas H. Meal
Ropes & Gray, LLP
One International Place
Boston, MA 02110

Dear Doug and Lydia:

I am writing in regard to your letter of January 13, 2012, in which you requested several internal FTC memoranda and other materials related to the FTC's investigation of your clients, Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, Wyndham Hotels & Resorts, LLC, and Wyndham Hotel Management, Inc. The content of your letter provides no basis for your request, and we are not aware of any legal requirement that the Commission produce such information. Accordingly, the Commission will not produce the requested documents. If you would like to discuss this further, please contact me at (202) 326-2276 or Lisa Schifferle at (202) 326-3377.

Best Regards,

A handwritten signature in black ink, appearing to read "Kristin Krause Cohen".

Kristin Krause Cohen
Attorney
Division of Privacy and Identity Protection



ROPES & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPESGRAY.COM

January 19, 2012

Douglas H. Meal
T +1 617 951 7517
F +1 617 235 0232
douglas.meal@ropesgray.com

BY EMAIL

Kristin Krause Cohen
Attorney, Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: In the Matter of Wyndham Hotels and Resorts –Federal Trade Commission File No.: 1023142

Dear Kristin:

Thank you for your letter of January 17, 2012. While we had thought that Wyndham's basis for requesting the documents identified in my January 13 letter was clear, we provide this letter as further clarification. The required memoranda by which Staff (i) sought authority to institute and/or expand the investigation described in the Access Letter (the "Staff Investigation"); (ii) asked that the Commission adopt the investigational resolution on which the CID ostensibly is predicated (i.e., the January 2008 resolution); and (iii) asked that the Commission issue the CID, and the documents by which the Commission and/or the Bureau Director acted on those requests, are potentially relevant to the propriety of Staff's actions in making those requests and the Commission's and/or the Bureau Director's actions in acting on those requests and hence are potentially relevant to the validity of the CID. Those documents are also potentially relevant to the authorized scope of the Staff Investigation and hence are potentially relevant to determining whether, and if so to what extent, the CID seeks information and documents that fall within that authorized scope.

As for the Commission's legal obligation to provide the documents Wyndham requested, those documents would be discoverable in any judicial proceeding to enforce the CID. Also, we cannot imagine why the Commission would want to keep those documents secret from Wyndham. So we assumed (and assume) that the Commission would be willing to provide the documents to

ROPES & GRAY LLP

Kristin Krause Cohen

- 2 -

January 19, 2012

Wyndham now, simply because it is the right thing for the Commission to do, under the circumstances.

Very truly yours,

A handwritten signature in black ink, appearing to read "Douglas H. Meal". The signature is stylized with a large, looped "D" and a horizontal line extending to the right, followed by a vertical line and a small hook at the end.

Douglas H. Meal

**WYNDHAM WORLDWIDE CORPORATION'S OBJECTIONS
TO THE FEDERAL TRADE COMMISSION'S
FIRST CIVIL INVESTIGATIVE DEMAND**

Pursuant to 15 U.S.C. § 57b-1(b)(13), Wyndham Worldwide Corporation (“WWC”) and Wyndham Hotels & Resorts LLC (“WHR”) (collectively, “Wyndham”), by and through their undersigned counsel, provide their objections to the first Civil Investigative Demand (“CID”) of the Federal Trade Commission (“FTC”) dated December 8, 2011 and served on December 12, 2011.

General Objections

1. Wyndham objects to the CID as overly broad, unduly burdensome, and oppressive.

2. Wyndham objects on the grounds that the Resolution attached to the CID Directing the Use of Compulsory Process in a Non-Public Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security (File No. P954807) is not specifically related to the FTC’s investigation of WHR and is not sufficient to authorize this CID.

3. Wyndham objects to the CID to the extent it seeks information or documents beyond the scope of, or seeks to impose obligations on Wyndham beyond those authorized by, the Resolution attached to the CID.

4. Wyndham objects to the CID to the extent it seeks information or documents that are not relevant to the question of whether WHR violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, or are not reasonably related to the FTC’s investigation of WHR.

5. Wyndham objects to the CID to the extent that the requests contained therein are too indefinite to constitute valid requests.

6. Wyndham objects to the CID to the extent that it seeks to impose any burden of production on or seeks any information regarding WWC, Wyndham Hotel Group (“WHG”), or Wyndham Hotel Management (“WHM”), as the sole target of the investigation is WHR.

7. Wyndham objects to the CID to the extent it seeks information or documents that are duplicative of information or documents previously provided to the FTC in the course of this investigation.

8. Wyndham objects to the CID to the extent that it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, the common interest privilege, the self-evaluative privilege, or any other applicable privilege or immunity.

9. Wyndham objects to the CID to the extent it seeks information, documents, data, or quantitative information not created or maintained in the ordinary course of business.

10. Wyndham objects to the CID to the extent it seeks information or documents over which WHR & Resorts, LLC does not have possession, custody, or control.

11. Wyndham objects to the CID to the extent it seeks information or documents the disclosure of which violates consumer or employee privacy rights.

12. The responses and objections of Wyndham to the CID are not intended as, and shall not be deemed as, an admission of the matters stated, implied, or assumed by or in the CID. No objection or limitation, or lack thereof, made in these responses and objections shall be deemed an admission by Wyndham as to the existence or non-existence of documents.

13. Wyndham provides these responses and objections without waiver of or prejudice to its right to raise objections at any later time to (a) any further demand or discovery relating to the matters raised in the CID, or (b) the relevance, materiality, or admissibility of the requests (or any part thereof), the statements made in this response (or any part thereof), or any documents produced pursuant to this response.

14. The following specific objections fully incorporated, are subject to, and are made without waiver of the foregoing general objections.

OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS

1. Wyndham objects to Definition E of “Company” as overly broad, unduly burdensome, and irrelevant to the extent it includes WWC, WHG, and WHM.

2. Wyndham objects to Definition J of “Document” to the extent it differs from the definition of “Document” as set forth in the Federal Rules of Civil Procedure and as unduly burdensome to the extent it requires Wyndham to collect and recover, restore, or produce Documents that exists on backup media or in other forms that are not reasonably accessible.

3. Wyndham objects to Definition L of “Electronically Stored Information” (“ESI”) to the extent it differs from the definition of “ESI” as set forth in the Federal Rules of Civil Procedure and as unduly burdensome to the extent it requires Wyndham to collect and recover, restore, or produce Documents that exist on backup media or in other forms that are not reasonably accessible.

4. Wyndham objects to Definition T of “Personal Information” as overly broad, irrelevant, and outside the scope of the FTC’s statutory authority because it includes information about employees, not just “consumers”, and to the extent it includes information about consumers that is neither confidential nor sensitive.

5. Wyndham objects to Definition Y of “Wyndham entity” as overly broad, unduly burdensome, and irrelevant to the extent it includes WWC, WHG, and WHM.

6. Wyndham objects to Instruction C regarding “Applicable Time Period” to the extent that it calls for the production of documents dated after May 1, 2010 as overly broad and unduly burdensome, as the FTC has not alleged that WHR committed any violations of the Federal Trade Commission Act after May 2010.

7. Wyndham objects to Instruction D regarding “Claims of Privilege” as unduly burdensome to the extent that it requires Wyndham to assert its claim of privilege prior to a meaningful review of its documents and to the extent it requires Wyndham to subject to a full schedule of items withheld.

8. Wyndham objects to Instruction I regarding “Scope of Search” as overly broad and unduly burdensome to the extent it seeks to require Wyndham to search the files of its attorneys or other third parties who are unlikely to possess unique relevant documents.

9. Wyndham objects to Instruction M regarding “Electronic Submission of Documents” to the extent it seeks to require Wyndham to produce documents in a format other than the format in which it has previously processed and produced documents as part of this investigation.

SPECIFIC OBJECTIONS

INTERROGATORIES

- 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 WHR, 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 WHM, and, if applicable, the date on which its management agreement was terminated.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR and to the extent the request seeks information that does not relate to any allegation that WHR violated the Federal Trade Commission Act. Wyndham further objects to Part (a) of this interrogatory as duplicative, as WHR has already provided this information with respect to WHR to the FTC during this investigation.

2. **Provide a high-level diagram (or diagrams) that sets out the components of each computer network used by WHR and WHM to store and process personal information, including any network hosted by WHR or WHM 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).**

Wyndham objects to this interrogatory as overly broad, unduly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information about WHM. Wyndham further objects to this interrogatory as duplicative to the extent it has already provided this information with respect to WHR to the FTC during this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request. Wyndham

further objects to the definition of personal information to the extent it includes data regarding employees and not consumers.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 4. Describe the process(es) used by WHR and WHM, 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; WHR or WHM; 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WHM. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 5. **Describe in detail Wyndham Worldwide’s role in the Information Security Programs of WHG, WHR, WHM, 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information with respect to WHR to the FTC during this investigation.

Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 6. Describe in detail WHG's role in the Information Security Programs of WHR, WHM, 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. WHG's role in developing and implementing each entity's Information Security Program;**
 - b. the training WHG provides to each entity related to the protection of personal information, including PCI DSS compliance;**
 - c. all policies, practices, and procedures relating to WHG'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. WHG'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 Hold Group's role in providing payment card authorization for each entity; and**

f. WHG employee(s) responsible for overseeing each entity's Information Security Program.

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information, with respect to WHGs' role in the information security function at WHR to the FTC during this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 7. Describe in detail WHR' role in the Information Security Programs of WHM, 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. WHR' role in developing and implementing each entity's Information Security Program;**
 - b. the training WHR provides to each entity related to the protection of personal information, including PCI DSS compliance;**
 - c. all policies, practices, and procedures relating to WHR' 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. WHR' 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. WHR' role in providing payment card authorization for each entity; and**
 - f. the WHR 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.**

Wyndham objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 8. Identify and describe in detail WHM'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. WHM's role in developing and implementing each hotel's Information Security Program;**
 - b. the training WHM provides to each hotel related to the protection of personal information, including PCI DSS compliance;**
 - c. all policies, practices, and procedures relating to WHM'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. WHM'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. WHM's role in providing payment card authorization for each hotel; and**
 - f. a list of all WHM employee(s) responsible for overseeing each hotel's Information Security Program.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WHM. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 9. Identify and describe in detail the 2009 decision that Wyndham Worldwide would assume responsibility from WHG for WHR's 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.**

Wyndham objects to this interrogatory as overly broad and unduly burdensome to the extent that it seeks to know “all reasons for the decision” and “any personnel changes”, as these facts may not be knowable to Wyndham at the present time and may have no relevance to the FTC’s investigation. Wyndham further objects to Part (c) of this interrogatory on the grounds that what constitutes a reason is vague and ambiguous. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during this investigation. Wyndham further objects to this interrogatory on the grounds that the meaning of the term "any other services" is vague and ambiguous. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent that WHR's relationship with its franchisees has no relevance to the question of whether WHR violated the Federal Trade Commission Act. Wyndham further objects to this interrogatory on the grounds that the meaning of the term "consequences" is vague and ambiguous.

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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information with respect to WHR to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request. Wyndham further objects to Parts (a)-(f) of this interrogatory as overly burdensome to the extent that it seeks to require Wyndham to provide a summary of information

that is not maintained regularly in any set of business records and for which responding would require the chronicling of email for a three-year period of time for a large number of employees at great time and expense. Wyndham further objects to this interrogatory on the grounds that the terms “practices”, “risk assessments”, “testing”, “monitoring”, “evaluation”, “procedures”, and “defenses” are vague and ambiguous. Wyndham further objects to this interrogatory to the extent it seeks information regarding the Wyndham-branded hotels that is not in the possession, custody, or control of Wyndham.

- 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 WHR’ 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory on the grounds that “risk assessment” is vague and ambiguous. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 14. For each WHR and WHM Service Provider:**

- a. **identify the Service Provider;**
- b. **identify the types of personal information that WHR and WHM 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as irrelevant, as the FTC has not alleged that WHR violated the FTC Act by employing any service provider who misappropriated personal information.

15. **Describe in detail the specific technical, administrative, and physical safeguards taken to re-architect and upgrade the WHR' 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 WHR' Phoenix data center environment from the Wyndham-branded hotel properties' networks;**
 - c. **expanding WHR' 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 WHR network;**
- g. **creating a holistic view of the WHR' environment; and**
- h. **any upgrades made to WHR' virus monitoring.**

Wyndham objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information with respect to WHR to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has

already provided the FTC with both narrative information and documents regarding entities that assisted it in relation to the data breaches previously identified by WHR during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 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).**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information, with respect to any data breaches of networks connected to the WHR network, to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation, to the extent this information is known or knowable to WHR. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request. Wyndham further objects to this interrogatory on the grounds that the meaning of “sanctions” is vague and ambiguous.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation, to the extent this information is known or knowable to WHR. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

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.

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this interrogatory as too indefinite to constitute a valid request.

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.

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information that is irrelevant to the question of whether WHR violated the FTC Act. Wyndham further objects to

this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this interrogatory as unduly broad and overly burdensome to the extent it seeks information that is irrelevant to the question of whether WHR violated the FTC Act. Wyndham further objects to this interrogatory as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation.

- 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.**

Wyndham objects to this interrogatory as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information

regarding WWC, WHG, and WHM other than their role in the information security operations of WHR, and to the extent the interrogatory seeks information that does not relate to any allegation that WHR violated the Federal Trade Commission Act, including, without limitation, information regarding records that may otherwise be irrelevant and records that were destroyed in the normal course of business prior to the anticipation of litigation. Wyndham further objects to this interrogatory as overly broad and unduly burdensome to the extent that Wyndham, WHG, WHR, and WHM did not create records in the ordinary course of business to document instances where its documents were destroyed and to the extent that the data necessary to create such records presently does not exist. Wyndham further objects to this interrogatory to the extent that records containing certain of the requested information were not created in the ordinary course of business, and data to create such records does not exist.

- 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.**

Wyndham objects to this interrogatory to the extent it seeks information protected by attorney-client or work product privilege.

- 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.**

Wyndham objects to this interrogatory as duplicative to the extent that WHR has already provided the FTC with an update regarding the information provided in the Access Letter Response.

II. DOCUMENTARY MATERIALS

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.**

Wyndham objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation.

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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent that it seeks information that is irrelevant to whether WHR violated the Federal Trade Commission Act. Wyndham further objects to this request as overly burdensome to the extent that records are not kept of documents provided to the Wyndham-branded hotels in the normal course of business and that responding to this request would require the review of the electronic files of a large number of Wyndham employees. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request to the extent it seeks documents not in the possession, custody, or control of WHR. Wyndham further objects to this request as too indefinite to constitute a valid request. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

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).

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent that WHR does not maintain records in the ordinary course of business that set forth the information sought by this request.

- 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent that WHR does not maintain records in the ordinary course of business that set forth the information sought by this request.

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 WHR's 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR and to the extent the request seeks information that does not relate to any allegation that WHR violated the Federal Trade Commission Act. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Subject to and without waiving the foregoing, WHR is willing to discuss narrowing this request with the FTC.

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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent that WHR does not maintain records in the ordinary course of business that set forth the information sought by this request.

- 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as unduly broad and overly burdensome to the

extent that production of “all documents” would require the review of electronic files for a large number of custodians at great time and expense. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent that WHR does not maintain records in the ordinary course of business that set forth the information sought by this request. Wyndham further objects to this request on the grounds that the terms “assess”, “evaluate”, “question”, “challenge”, “contest the effectiveness”, “verifies”, “confines”, “challenges”, “questions”, or “otherwise concerns” are vague and ambiguous. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

- 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request to the extent it seeks production of documents not in the possession, custody, or control of Wyndham. Wyndham further objects to this request on the grounds that the terms “policies”, “procedures”, or “practices” are vague and ambiguous.

- 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).

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as unduly broad and overly burdensome to the extent that production of "all documents" would require the review of electronic files for a large number of custodians at great time and expense. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent it seeks production of documents not in the possession, custody, or control of Wyndham. Wyndham further objects to this request on the grounds that the terms "identify", "describe", "investigate", "evaluate", or "assess" are vague and ambiguous. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

- 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as unduly broad and overly burdensome to the extent that production of “all documents” would require the review of electronic files for a large number of custodians at great time and expense. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent it seeks production of documents not in the possession, custody, or control of Wyndham. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as unduly broad and overly burdensome to the extent that production of "all documents" would require the review of electronic files for a large number of custodians at great time and expense. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent it seeks production of documents not in the possession, custody, or control of Wyndham. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further

objects to this request to the extent it seeks production of documents not in the possession, custody, or control of Wyndham. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

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.

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as unduly broad and overly burdensome to the extent that production of “all documents” would require the review of electronic files for a large number of custodians at great time and expense. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects to this request to the extent it seeks production of documents not in the possession, custody, or control of Wyndham. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

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.**

Wyndham objects to this request as duplicative to the extent that WHR has already provided this information to the FTC during the course of this investigation. Wyndham further objects to this request as overly burdensome and not reasonably calculated to lead to the discovery of admissible evidence to the extent the request seeks information that does not relate to any allegation that WHR violated the Federal Trade Commission Act. Wyndham further objects to this request as too indefinite to constitute a valid request.

- 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham objects to this request as duplicative to the extent that WHR has already provided this information with respect to WHR to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request.

- 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.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as unduly broad and overly burdensome to the extent that production of “all documents” would require the review of electronic files for a large number of custodians at great time and expense. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information with respect to WHR to the FTC during the course of this investigation. Wyndham further objects to this request as too indefinite to constitute a valid request. Wyndham further objects on the grounds that the term “actual or potential harm to consumers” is vague and ambiguous. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

17. **All contracts and memoranda relating to the transfer of information security responsibilities for WHR from WHG to Wyndham Worldwide, and all contracts between any Wyndham entities relating to responsibility for information security.**

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as too indefinite to constitute a valid request. Subject to and without waiving the foregoing, WHR is willing to discuss a limited custodian approach to responding to this request with the FTC.

18. All minutes of Board of Directors meetings, executive committee meetings, or audit committee meetings of each Wyndham entity during the applicable time period.

Wyndham objects to this request as overly burdensome and not reasonably calculated to lead to the discovery of admissible evidence to the extent the request seeks information that does not relate to any allegation that WHR violated the Federal Trade Commission Act. Subject to and without waiving the foregoing, WHR is willing to discuss narrowing this request with the FTC.

19. Documents sufficient to show the Company's policies and procedures relating to the retention and destruction of documents.

Wyndham objects to this request as unduly broad, overly burdensome, and not reasonably calculated to lead to the discovery of admissible evidence to the extent it seeks information regarding WWC, WHG, and WHM other than their role in the information security operations of WHR. Wyndham further objects to this request as duplicative to the extent that WHR has already provided this information with respect to WHR to the FTC during the course of this investigation.

Wyndham Worldwide Corporation
and Wyndham Hotels & Resorts, LLC

By Their Attorneys

/s/ Douglas H. Meal
Douglas H. Meal, Esq.
Ropes & Gray LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

Seth C. Silber, Esq.
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW
Fifth Floor
Washington, DC 20006
(202) 973-8800

Date: January 20, 2012



Office of the Secretary

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

April 11, 2012

VIA EMAIL AND COURIER DELIVERY

Seth Silber, Esq.
Wilson Sonsini Goodrich & Rosati
1700 K Street, N.W.
Fifth Floor
Washington, D.C. 20006-3817
ssilber@wsgr.com

Douglas H. Meal, Esq.
Ropes & Gray, LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
douglas.meal@ropesgray.com

RE: Petition of Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation to Quash, or Alternatively, Limit Civil Investigative Demand

Dear Messrs. Silber and Meal:

On January 20, 2012, the Federal Trade Commission (“FTC” or “Commission”) received the petition filed by Wyndham Hotels and Resorts (“WHR”) and its parent company Wyndham Worldwide Corporation (“WWC,” and collectively with WHR, “Wyndham,” or “Petitioners”). This letter advises you of the Commission’s disposition of the petition, effected through this ruling by Commissioner Julie Brill, acting as the Commission’s delegate.¹

For the reasons explained below, the petition is granted as to modifying the definition of personal information and one CID Instruction and denied in all other respects. The documents and information required by the CID must now be produced on or before April 23, 2012, consistent with modifications to the CID definitions and instructions described below. You have the right to request review of this ruling by the full Commission.² Any such request must be filed with the Secretary of the Commission within three days after service of this letter ruling.³ The timely filing of a request for review of this ruling by the full Commission does not stay the return dates established by this ruling.⁴

¹ See 16 C.F.R. § 2.7(d)(4).

² 16 C.F.R. § 2.7(f).

³ *Id.* This letter ruling is being delivered by e-mail and courier delivery. The e-mail copy is provided as a courtesy, and the deadline by which an appeal to the full Commission would have to be filed should be calculated from the date on which you receive the original letter by courier delivery.

⁴ *Id.*

PUBLIC

I. INTRODUCTION

In early 2010, WHR disclosed that an intruder or intruders had gained access to its computer networks and to networks belonging to independently-owned Wyndham-branded hotels. Later press reports indicated that breaches of its computer network occurred on three occasions between July 2008 and January 2010.⁵ Among the information compromised in these repeated breaches were payment cards for more than 619,000 people.⁶ The exposure of this information can result in harms including identity theft, financial fraud, and the basic inconvenience of replacing stolen card numbers.⁷

In response, on April 8, 2010, FTC staff commenced an investigation and delivered to WHR a voluntary request for information (“Access Letter”) that included both interrogatories and document requests. Though the letter was addressed to an official at WHR, the letter defined “Wyndham” to include not only WHR but also “its parents, subsidiaries, affiliates, franchisees, hotels managed by franchisees that use the Wyndham trade name, and agents.”⁸ After discussions, staff and WHR agreed to limit an initial production to two custodians, although staff reserved the right to identify additional custodians based on the materials produced. The letter called for a response by May 10, 2010, but WHR did not respond to the interrogatories until July 19, 2010, and did not complete production of documents until October 2010.

Upon review, staff identified deficiencies in the production, most notably that WHR produced a large number of completely irrelevant and nonresponsive materials. WHR also failed to produce information that was obviously relevant to the investigation, such as supporting documents and information referenced in forensic reports that the company did provide.

In November 2010, Commission staff informed WHR of these deficiencies and the need to obtain documents from additional custodians. During these negotiations, WHR expressed an interest in pursuing settlement. The company stated, however, that it could not respond to the Access Letter and negotiate settlement simultaneously, and it asked staff to suspend the document collection. In January 2011, staff agreed to do so, but informed WHR that it reserved the right to demand resumption of document collection and to pursue additional custodians should settlement discussions fail.

⁵ Pet., Exh. 3, at 1 n.1.

⁶ See, e.g., Pet. Exh. 5, at 4 (proposed complaint).

⁷ See, e.g., *Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 3-4, 10 (2005) (statement of Deborah Platt Majoras, Chairman of the Federal Trade Commission).

⁸ Pet., Exh. 3, at 2.

Staff pursued settlement discussions with WHR over the next nine months. Staff and WHR were unable to reach settlement terms, and on September 19, 2011, WHR informed staff it would not enter into a settlement on the terms staff proposed.

Accordingly, in September 2011, staff informed WHR that it would resume the investigation. Soon thereafter, WHR agreed to provide a certification as to the completeness of the materials it had produced to date in response to the Access Letter. WHR provided this certification on December 1, 2011.

The FTC issued a CID to WHR on December 8, 2011 pursuant to Resolution P954807, a “blanket resolution” issued by the Commission on January 3, 2008. This Resolution authorizes FTC staff to use compulsory process in investigations

[t]o 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.⁹

II. ANALYSIS

A. The CID was lawfully issued and Petitioners have sufficient notice of the nature and scope of the investigation.

Petitioners’ principal objection, which they restate in various ways, is that the CID and its authorizing resolution are deficient for failing to inform them sufficiently of the nature and scope of the investigation. We find this complaint not credible, coming as it does nearly two years after the investigation commenced. As the petition acknowledges, there have been substantial ongoing communications since FTC staff first contacted Petitioners in April 2010. As Petitioners readily admit, they have already reviewed and produced over one million pages of documents at significant expense; presumably, Petitioners did not do so without some understanding of why those documents had been requested.¹⁰ Moreover, Petitioners admit that the “CID did not come as a surprise[,]” because they undertook to certify their prior productions in anticipation.¹¹ Indeed, staff presented Petitioners with a draft complaint, Petitioners responded with a 60-page

⁹ Pet., Exh. 1.

¹⁰ Pet., at 35.

¹¹ *Id.*, at 10.

“white paper,” and both parties have engaged in detailed and lengthy settlement negotiations.¹² In light of these facts, we find that the nature and scope of the investigation are quite clear to Petitioners and consequently that their claim of insufficient notice is specious.¹³

More important, it is well-established that a CID is proper if it “state[s] the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.”¹⁴ In the present matter, we find that the authorizing resolution adequately delineates the purpose and scope of the investigation: “[t]o 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” (emphasis added). The description of the subject matter of the investigation, coupled with a citation to the statutory prohibition on “unfair or deceptive acts or practices” satisfies that requirement.¹⁵ This has put WHR on notice as to the purpose, scope, and legal basis for the Commission’s investigation. There is no need to either state the purpose of an investigation with greater specificity, or tie the conduct under investigation to any particular theory of violation.¹⁶

¹² *Id.*, at 7-9 and Exh. 7.

¹³ *Cf. Assocs. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) (“In sum, the notice provided in the compulsory process resolutions, CIDs, and other communications with Petitioners more than meets the Commission’s obligation of providing notice of the conduct and the potential statutory violations under investigation.”).

¹⁴ 15 U.S.C. § 57b-1(c)(2). *See also* 16 C.F.R. § 2.6.

¹⁵ *FTC v. O’Connell Assoc.*, 828 F. Supp. 165, 170-71 (E.D.N.Y. 1993) (quoting *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992)); *see also FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980). Petitioners attempt to distinguish *O’Connell* on the grounds that the resolution in that case was an omnibus resolution, not a blanket one, and it was used on the basis of a tip to authorize compulsory process to a new recipient as part of an ongoing investigation. The issue of whether a resolution is blanket or omnibus is not relevant because either is an acceptable form of resolution. Furthermore, the resolution upheld in *O’Connell* stated only that the nature and scope of that investigation involved Section 5 and the Fair Credit Reporting Act. *O’Connell*, 828 F. Supp. at 167 & n.1. This description is at least as specific as “consumer privacy and/or data security,” the description at issue here. Finally, just as in *O’Connell*, the CID here was issued as part of a pre-existing, ongoing investigation. In fact, considering the history of the investigation before the CID was issued, Petitioners here had far greater information about what staff was investigating than did *O’Connell Associates*.

¹⁶ *Invention Submission*, 965 F.2d at 1090; *FTC v. National Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (citing *EPA v. Alyeska Pipeline Serv. Co.*, 836 F.2d 443, 477 (9th Cir. 1988)).

Moreover, contrary to Petitioners' contention, the resolution is not invalid because it is a so-called "blanket resolution." According to Petitioners, Sections 2.4 and 2.7 of the Commission's Rules of Practice, 16 C.F.R. §§ 2.4, 2.7, require resolutions to be tailored to the facts of each investigation.¹⁷ But no such requirement arises under the Commission's Rules. Rule 2.4 states that the Commission "may, in any matter under investigation adopt a resolution authorizing the use of any or all of the compulsory processes provided for by law."¹⁸ That provision does not require a separate investigational resolution for each investigation, as Petitioners seem to suggest.¹⁹ Likewise, Rule 2.7 simply states that the Commission may, pursuant to a resolution, issue compulsory process for documents or testimony.²⁰ This rule does not address the contents or form of the authorizing resolution. Accordingly, the resolution in this case satisfies the Commission's Rules.²¹

¹⁷ Pet., at 16-18 (citing 16 C.F.R. §§ 2.4, 2.7).

¹⁸ 16 C.F.R. § 2.4.

¹⁹ The narrowly tailored resolution that Petitioners desire is known as a "special resolution," and is one of three possible types suggested for FTC staff in the Commission's Operating Manual. See FTC Operating Manual, Chapter 3.3.6.7.4.1 to 3.3.6.7.4.4. The Commission has repeatedly rejected the proposition that such specificity is required in every investigation. See, e.g., *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010) ("The Commission is not required to identify to Petitioners the specific acts or practices under investigation"), available at <http://www.ftc.gov/os/quash/100712hortonresponse.pdf>; *Dr. William V. Judy*, No. X000069, at 4-5 (Oct. 11, 2002) (sustaining validity of CIDs issued pursuant to an omnibus resolution), available at <http://www.ftc.gov/os/quash/021011confirmanthonyltr.pdf>; *In re Assocs. First Capital Corp.*, 127 F.T.C. at 914 ("[R]ecitation of statutory authorities provides adequate notice to Petitioner as to [the] purposes of the investigation."). To the extent that courts have considered the issue, they also have rejected the proposition that the Commission is so constrained. *FTC v. National Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2; *O'Connell*, 828 F. Supp. at 170-71.

²⁰ 16 C.F.R. § 2.7(a).

²¹ Petitioners also contend that the resolution fails to conform to the FTC's Operating Manual. Pet., at 17-18. However, the sufficiency of staff's compliance with the Operating Manual is of no concern to Petitioners because the Operating Manual confers no rights on them. See FTC Operating Manual, Chapter 1.1.1 ("Failure by the staff or the Commission to adhere to procedures outlined by this Operating Manual does not constitute a violation of the Rules of Practice nor does it serve as a basis for nullifying any action of the Commission or the staff.") See also *FTC v. Nat'l Bus. Consultants, Inc.*, 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶ 68,984, at *29 (E.D. La. 1990) (reading Chapter 1.1.1 to find that the Operating Manual was "not binding").

Petitioners also challenge the resolution as insufficiently specific in light of the legislative history of the Federal Trade Commission Improvements Act of 1980, which added a new Section 20 of the FTC Act.²² Petitioners allege that this legislative history shows that Congress intended the FTC to provide more than “a vague description of the general subject matter of the inquiry . . .[.]”²³ and that the resolution here does not meet Congress’s expectations.

We reject this argument for the same reason we rejected Petitioners’ other arguments: the Commission’s resolution satisfies the requirements of the statute.²⁴ It informs Petitioners of the nature of the conduct constituting the alleged violation—unfair or deceptive acts or practices involving consumer privacy and/or data security—and it identifies the applicable provision of law—Section 5 of the FTC Act. Moreover, even as Congress expressed its desire for specific notice, it nonetheless cautioned against reading too much into Section 20: “[T]his requirement is not intended to be overly strict so as to defeat the purpose of the act or to breed litigation and encourage the parties investigated to challenge the sufficiency of the notice.”²⁵ We find that the resolution meets all legal requirements.²⁶

Finally, Petitioners claim that the CID exceeded the FTC’s jurisdiction by requesting information about employees, a group it contends is distinct from “consumers” for purposes of Section 5. Pet., at 28-32. We need not entertain this claim because challenges to the FTC’s jurisdiction or regulatory coverage are not properly raised through challenges to investigatory process. *See, e.g., FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (citing *United States v. Sturm, Ruger & Co.*, 84 F.3d 1, 5 (1st Cir. 1996)). However, we choose to adopt this modification because staff already offered to modify the CID definitions to exclude employee information. Pet., Exh. 11, at 3.

²² Pet., at 18, 20-21, 24.

²³ S. Rep. No. 96-500, at 23 (1979).

²⁴ *See* 15 U.S.C. 57b-1(c)(2) (“Each civil investigative demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.”); *see also O’Connell*, 828 F. Supp. at 170-71; *Dr. William V. Judy*, No. X000069, at 4-5 (rejecting a challenge to a resolution based on the legislative history of Section 20), *available at* <http://www.ftc.gov/os/quash/021011confirmanthonyltr.pdf>.

²⁵ S. Rep. No. 96-500, at 23 (1979).

²⁶ *Ken Roberts Co.*, 276 F.3d.

B. The CID is not overbroad, unduly burdensome, or indefinite.

Petitioners also advance a series of arguments about the CID specifications, claiming that the CID is overbroad and asks for information not reasonably related to the investigation, in particular, information related to WHR’s corporate parent WWC and its affiliates.²⁷

An administrative subpoena is valid if the requested information is “reasonably relevant” to the purposes of the investigation.²⁸ Reasonable relevance is defined broadly in agency law enforcement investigations. As the D.C. Circuit has stated, “The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one The requested material, therefore, need only be relevant to the *investigation*—the boundary of which may be defined quite generally, as it was in the Commission’s resolution here.”²⁹ Courts thus place the burden on Petitioners to show that the Commission’s determination is “obviously wrong” and that the information is irrelevant.³⁰

Here, as Petitioners admit, Commission staff provided an explanation of the relevance of these requests.³¹ More generally, staff’s investigation focuses on a series of breaches of WHR’s data security processes that are managed by other Wyndham entities.³² In light of this, CID specifications that probe the details of the information security systems developed by Petitioners and their affiliates are relevant to this investigation. Petitioners have not met their burden of showing that this information is irrelevant, or that the Commission’s request for it is “obviously wrong.”

²⁷ Pet., at 33-36.

²⁸ *Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. RTC*, 5 F.3d 1508, 1516 (D.C. Cir. 1993) (citing *Invention Submission Corp.*, 965 F.2d at 1089; *FTC v. Anderson*, 631 F.2d 741, 745 (D.C. Cir. 1979); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977)).

²⁹ *Invention Submission Corp.*, 965 F.2d at 1090 (emphasis in original; internal citations omitted) (citing *Carter*, 636 F.2d at 787-88, and *Texaco*, 555 F.2d at 874 & n. 26).

³⁰ *Invention Submission Corp.*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) (“The burden of showing that the request is unreasonable is on the subpoenaed party.”); *Texaco*, 555 F.2d at 877 n.32. *Accord FTC v. Church & Dwight Co., Inc.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010).

³¹ Pet., at 33 (citing Pet., Ex. 11, at 2).

³² Pet., Exh. 11, at 2.

Petitioners further claim the CID is unduly burdensome, for the following reasons: (1) they have already spent over \$5 million in responding, including producing over one million pages, and staff should now have enough information; (2) responding to the interrogatories will require six months and significant additional costs; (3) responding to the document requests that ask for “all documents” relating to a given subject will require about 10 weeks and \$1 million to produce documents from an additional three custodians; and (4) responding to the document requests that ask for “documents sufficient to identify” a given subject are “hugely burdensome” and will require 6 months and \$2.75 million to produce documents from the same three custodians. In sum, Petitioners claim that responding to the CID will require an additional \$3.75 million, on top of what they have spent to date, and 1 to 2 years’ additional time.³³

Of course, the recipient of a CID must expect to incur some burden in responding to a CID.³⁴ The responsibility of establishing undue burden rests on Petitioners,³⁵ who must show that compliance threatens to seriously impair or unduly disrupt the normal operations of their business.³⁶ Likewise, a CID is not unreasonably broad where the breadth of the inquiry is in large part attributable to the magnitude or complexity of the subject’s business operations.³⁷ Petitioners’ estimate is not insubstantial, but we find that they have not sustained their burden.

First, Petitioners’ estimate is neither specific nor detailed and does not account for factors that may reduce the cost and time of production. For one, Petitioners have not sufficiently addressed the availability of e-discovery technology, such as advanced analytical tools and predictive coding, to enable fast and efficient search, retrieval, and production of electronically stored information (ESI).³⁸ While Petitioners do tally the potential costs of an ESI production and refer to a vendor, these costs are unsupported by any detailed breakdown or itemization.³⁹

³³ Pet., at 36-39; *see also* Pet., Exh. 4, at 2-4.

³⁴ *See FTC v. Shaffner*, 626 F.2d 32, 38 (7th Cir. 1980); *Texaco*, 555 F.2d at 882.

³⁵ *See Texaco*, 555 F.2d at 882; *In re Nat’l Claims Serv., Inc.*, 125 F.T.C. 1325, 1328-29 (1998). *See also EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986); *FTC v. Standard American, Inc.*, 306 F.2d 231, 235 (3d Cir. 1962) (appellants have the burden to show unreasonableness of the Commission’s demand and make a record to show the “measure of their grievance rather than [asking the court] to assume it”) (citing *Oklahoma Press Publ’g Co. v. Walling*, 327 U.S. 186, 217-18 (1946); *United States v. Morton Salt Co.*, 338 U.S. 632, 654 (1950)).

³⁶ *See Shaffner*, 626 F.2d at 38; *Texaco*, 555 F.2d at 882.

³⁷ *See Texaco*, 555 F.2d at 882.

³⁸ *See, e.g., Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 318 (S.D.N.Y. 2003) (Sheindlin, J.) (“Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks,

Petitioners' estimate also does not account for the effect of Instruction K, which permits Petitioners to identify, without having to reproduce, documents that were previously provided to the Commission.⁴⁰ To the extent that Petitioners' cost estimate includes production of duplicate materials, Instruction K permits Petitioners to avoid this expense and reduces the potential burden. Though Petitioners respond that staff, and not they, should bear the burden of avoiding duplicative document requests,⁴¹ Petitioners are the ones with the most information about their document collections and productions to date. In fact, Petitioners have already identified the areas of overlap between the Access Letter and the CID.⁴² The Access Letter instructed Petitioners to identify which of the documents produced answered the specifications in the Access Letter.⁴³ It is not unduly burdensome for Petitioners to compare their Access Letter response with the CID to identify duplicates.

and the production can be made in electronic form obviating the need for mass photocopying.”); John Markoff, *Armies of Expensive Lawyers, Replaced by Cheaper Software*, NEW YORK TIMES, Mar. 5, 2011, at A1, *available at*, <http://www.nytimes.com/2011/03/05/science/05legal.html>).

³⁹ Pet., Exh. 4, at 2-4. The lack of factual support for the claim of undue burden is underscored by the fact that the estimated costs appear out of proportion to the number of custodians involved. According to the declaration from Korin Neff, WHR spent approximately \$2.5 million *per custodian* for its first production, and now estimates that it will spend approximately another \$3.75 million for three custodians, or \$1.25 million *per custodian*, in response to the CID. *Id.* One explanation for the cost of the production to date may be the fact that WHR produced a large number of irrelevant and nonresponsive materials, including, among others, multiple copies of third party software licenses, in various languages; numerous magazines and newsletters not specific to WHR; and, human resources materials. This may explain why WHR could generate more than one million pages from only two individuals.

⁴⁰ Pet., Exh. 1, at 7 (“K. 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.”).

⁴¹ Pet., at 39.

⁴² See Pet., Exh. 2, at Exhs. C, D. As Petitioners point out, WHR has already responded to 42 out of the 89 interrogatories and subparts in the CID, and 25 of the 38 document requests and subparts. Pet., Exh. 2, at 2.

⁴³ See Pet., Exh. 3, at 2 (“Please Bates stamp your response and itemize it according to the numbered paragraphs in this letter.”).

Second, Petitioners have not established that this will seriously disrupt their operations. As expressed in *Texaco* and other key cases, some cost to recipients of process is expected, and the burden posed by this cost is evaluated in relation to the size and complexity of a recipient's business operations. In *Texaco*, for instance, the court affirmed enforcement of a subpoena that the company claimed would require 62 work-years and \$4 million for compliance.⁴⁴ As in that case, it appears that the burden here may be a consequence of size—in 2010, Wyndham had an annual revenue of more than \$3.8 billion—as well as the complexity of the corporate structure Wyndham has adopted.⁴⁵ Thus, full compliance with the CID, even if it were to reach the estimates included in the petition, is unlikely to “pose a threat to the normal operation of” Wyndham “considering [its] size.”⁴⁶

Third, Petitioners have claimed that the requests that ask for documents “sufficient to describe” the subject of the request present a “huge cost” and “extreme burden,” particularly because the companies do not keep records in the manner called for.⁴⁷ It is unclear why a request that calls for documents “sufficient to describe” should be more burdensome than a request that calls for “all documents”; by definition, documents “sufficient to describe” should involve fewer than “all documents.” The fact that Petitioners do not keep records in the manner that matches the request is not unusual and by itself does not present a basis for quashing these requests. Because staff often does not know how a CID recipient keeps its records, staff crafts its requests broadly, but provides a recipient flexibility in responding by allowing the recipient to produce those documents “sufficient to describe.”

Fourth, the fact that Petitioners have already produced information to staff does not establish either that staff has sufficient information, or that further requests are unduly burdensome. The obligation is on Petitioners to show that the CID is unduly burdensome, not on staff to show that the CID is necessary.⁴⁸

⁴⁴ *Texaco*, 555 F.2d at 922 (Wilkey, J., dissenting).

⁴⁵ Wyndham Worldwide Corp., Annual Report (Form 10-K), at 34 (Feb. 22, 2011).

⁴⁶ *FTC v. Rockefeller*, 591 F.2d 182, 190 (2d Cir. 1970).

⁴⁷ Pet., at 38-39. *See also* Pet., Exh. 10, at 6.

⁴⁸ *Cf. United States v. AT&T, Inc.*, No. 1:11-cv-01560, 2011 WL 5347178, at *6 (D.D.C. Nov. 6, 2011) (“There is no requirement that AT&T demonstrate to Sprint’s satisfaction that the legal theories AT&T wishes to consider require documents beyond those [Sprint previously] supplied to DOJ . . .”).

Fifth, we find that Petitioners have not sufficiently availed themselves of the meet-and-confer process required by the FTC's Rules of Practice and the CID itself.⁴⁹ As we have previously said, this meet-and-confer requirement "provides a mechanism for discussing adjustment and scheduling issues and resolving disputes in an efficient manner."⁵⁰ Thus, the meet-and-confer requirements offer a critical opportunity for the recipient of a CID to engage with staff in a meaningful discussion aimed at reducing the burden of compliance. Here, Petitioners did not engage in a good faith exchange with staff intended to identify and discuss issues of burden.⁵¹ Instead, Petitioners raised many of the same arguments found in this petition, often verbatim, and did not respond to legitimate requests from staff for specific proposals for narrowing or limiting the CID's scope. While staff was apparently willing to compromise on several issues, Petitioners demanded blanket and arbitrary caps on the number of document requests, interrogatories, and custodians. Petitioners cannot claim undue burden when they themselves undertook an inadequate meet-and-confer with staff.

Despite Petitioners' failure to carry their burden, we conclude that some modifications to the CID instructions may lessen Petitioners' costs of compliance. Accordingly, we amend the instructions to permit Petitioners to submit documents in lieu of interrogatories. This modification will allow Petitioners to avoid the time and expense of preparing interrogatory responses. In addition, to the extent that a document may be responsive to multiple interrogatories or document requests, Petitioners need not produce multiple copies but, pursuant to Instruction K, discussed above, may produce one copy of a relevant document, and then indicate each specification or interrogatory to which the document is responsive. This should mitigate the costs of compliance.

Finally, Petitioners argue that the CID is indefinite. This claim appears to restate several of Petitioners' other objections, including their claim of a lack of notice of the purpose and scope of the investigation, overbreadth, and burden.⁵² For the reasons discussed above, this claim of indefiniteness is without basis.

⁴⁹ 16 C.F.R. § 2.7(d)(2); Pet. Exh. 1, at 5.

⁵⁰ *Firefighters Charitable Found., Inc.*, FTC File No. 102-3023, at 3 (Sept. 23, 2010).

⁵¹ *See* Pet. Exhs. 9-15.

⁵² Pet., at 39-40.

C. The CID was not issued for an improper purpose.

Petitioners claim that the size and timing of the CID shows that its true purposes were either to coerce settlement, or to obtain discovery outside of the rules of civil procedure. The facts of the investigation refute this conclusion. Mid-investigation, Petitioners expressed an interest in exploring settlement talks as a means of resolving the matter short of a full-blown investigation and consequent possible law enforcement action. At Petitioners' request, staff voluntarily allowed them to suspend their production, in order to reduce the burden on Petitioners. But staff also advised Petitioners that they would resume their investigation should settlement talks fail. And, as Petitioners admit, when the CID was issued, it was no surprise.⁵³ In light of these circumstances, there is no evidence of improper purpose, either to coerce settlement or to obtain information outside of the information necessary to complete the investigation.

III. CONCLUSION AND ORDER

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** the Petition of Wyndham Hotels & Resorts and Wyndham Worldwide Corporation to Quash, or Alternatively, Limit Civil Investigative Demand be, and it hereby is, **DENIED IN PART AND GRANTED IN PART.**

IT IS FURTHER ORDERED THAT the Definition T, "Personal information," be amended to exclude employee information as follows:

"Personal information" shall mean individually identifiable 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) e-mail address or other online contact information, such as instant messenger 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) 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 (9) any information from or about an individual consumer that is combined with any of (1) through (8) above.

⁵³ *Id.*, at 10.

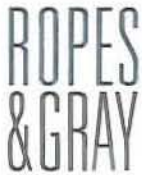
IT IS FURTHER ORDERED THAT the CID Instructions be modified to include the following instruction:

“Q. Submission of Documents in lieu of Interrogatory Answers: Previously existing documents that contain the information requested in any written Interrogatory may be submitted as an answer to the Interrogatory. In lieu of identifying documents as requested in any Interrogatory, you may, at your option, submit true copies of the documents responsive to the Interrogatory, provided that you clearly indicate the specific Interrogatory to which such documents are responsive.”

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demand to Wyndham Hotels & Resorts and Wyndham Worldwide Corporation must now be produced on or before April 23, 2012.

By direction of the Commission.

Donald S. Clark
Secretary



ROPE & GRAY LLP
PRUDENTIAL TOWER
800 BOYLSTON STREET
BOSTON, MA 02199-3600
WWW.ROPEGRAY.COM

January 13, 2012

Douglas H. Meal
T +1 617 951 7517
F +1 617 235 0232
douglas.meal@ropesgray.com

BY EMAIL

Kristin Krause Cohen, Esq.
Division of Consumer Privacy and Protection
Bureau of Consumer Protection
601 New Jersey Avenue NW
Washington, DC 20580

Re: In the Matter of Wyndham Hotels and Resorts –Federal Trade Commission File No.: 1023142

Dear Kristin:

Thank you for your January 12, 2012 letter regarding the Federal Trade Commission's ("FTC") Civil Investigative Demand to Wyndham Worldwide Corporation ("CID").

Without commenting at this juncture on any of the other statements in your letter, we note that your letter proposes further discussion in an effort to resolve Wyndham's objections to the CID. We would be glad to continue to discuss these issues with the FTC. However, as you are aware, for the next week, Wyndham and its counsel are fully engaged in drafting our anticipated petition to quash, which is due on January 20, 2012. Accordingly, unless the Staff is willing to extend the deadline for filing the petition so as to allow further discussions regarding Wyndham's objections to the CID to occur, any such discussions will have to occur after January 20.

Very truly yours,

Douglas H. Meal

cc: Lydia Parnes
cc: Lisa Schifferle


SUPPLEMENTAL 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” or “Commission”) investigation (the “WHR Investigation”) that is the subject of the petition to quash and this request for review of Commissioner Julie Brill’s April 11, 2012 letter ruling (the “Letter Ruling”) denying said petition. I make this declaration in support of this request for review by the full Commission (the “Appeal”) of the Letter Ruling. 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 factual matters referenced in the Appeal pertaining to the WHR Investigation. Each of the factual statements in the Appeal regarding the WHR Investigation is accurate to the best of my knowledge, information, and belief.

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



Douglas H. Meal

Executed on April 20, 2012