UNITED STATES DISTRICT COURT.
FOR THE DISTRICT OF NEW JERSEY
Civil 13-1887 ES

FEDERAL TRADE COMMISSION,

Plaintiff, MOTIONS TO DISMISS

V.

WYNDHAM WORLDWIDE CORPORATION, ET AL,

DEFENDANTS.

- -

NEWARK, NEW JERSEY
NOVEMBER 7, 2012

B E F O R E: HONORABLE ESTHER SALAS,
UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S:

KEVIN HYLAND MORIARTY, ESQ.
KRISTIN KRAUSE COHEN, ESQ.
JONATHAN ELI ZIMMERMAN, ESQ.
FOR THE FEDERAL TRADE COMMISSION.

GIBBONS
BY: JUSTIN T. QUINN, ESQ.
AND
KIRKLAND & ELLIS
BY: EUGENE ASSAF, ESQ.
AND: K. WINN ALLEN, ESQ.
For the Defendants.

Pursuant to Section 753 Title 28 United States Code, the following transcript is certified to be an accurate record as taken stenographically in the above-entitled proceedings.

S/LYNNE JOHNSON

- -

LYNNE JOHNSON, CSR, CM, CRR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT
P.O. BOX 6822
LAWRENCEVILLE, NEW JERSEY 08648
CHJLAW@AOL.COM

THE COURT: Good morning to everyone. Please be seated.

We are on the record in the matter of Federal Trade Commission versus Wyndham Worldwide Corporation et al, civil 13-1887. Let me have appearances by counsel.

MR. MORIARTY: Kevin Moriarty on behalf of the Federal Trade Commission.

MR. ZIMMERMAN: Jonathan Zimmerman on behalf of the Federal Trade Commission.

MS. COHEN: Kristin Cohen for the FTC.

MR. QUINN: Justin Quinn for the defendants. Along with me at counsel table is Eugene Assaf, K. Winn Allen and Douglas Meal. Also with me are representatives from Wyndham, Marcus Banks and Korin Neff.

Mr. Assaf will be arguing the authority question. Mr. Allen will be answering any questions with respect to the common enterprise and if your Honor has any questions on the motion to stay, I will be addressing those.

THE COURT: Perfect. Be seated.

Let me tell you the order we are going to go today. We are going to start with whether Section 5, unfair authority extends to data security and if so,

does it govern the security of payments, payment card data. So what we are going we are going to deal first as it was in the briefs. Count 2, the unfairness claim.

Let's deal with the first issue, whether again, as I said a moment ago, Section 5 unfairness authority extends to data security, and issue two then will be whether the FTC is required to provide fair notice of what Section 5 requires.

And then issue three will be whether unfairness is adequately pled by the plaintiffs.

We then will move to the second argument, count 1, which is the deception claim, and we will have argument on that claim. Then at some point we will probably break. We will come back and we will deal with the other Wyndham entities' motions to dismiss and finally we will deal with the motion to stay discovery. That is the order in which we will be conducting argument today.

Let's start with, it is the first issue, I would like to open with defendants.

Counsel, I know that you feel that Section 5, the unfair authority, extends to data security. You do not believe it does. I will hear from you now.

Let me apologize in advance to counsel. I

tend to ask a lot of questions. I tend to interrupt counsel, when they are speaking and it is not meant to be rude.

I just want to get to the issues that I am wrestling with, having prepared for this hearing today.

So I will let you start, counsel, but your fairy provided fair warning that we are going to have a number of questions for you.

MR. ASSAF: Gene Assaf on behalf of Wyndham.

Thank you, your Honor, for the time and quite clearly the attention you are devoting. I also thank you for your warning, but I will say having done this now for 25 years, it is a pleasure to be in front of a litigator because I will be ready to hear your questions.

I know when you have them you will fire them. Hopefully I will have some answers for you.

Your Honor, as an initial matter, before we start, in order to assist the Court and quite frankly to assist the parties, what my practice is, and I would ask permission to approach the Court and the clerks. I have a deck that will we will run through. I think I have ordered it in the same order as your Honor, so we would start at the beginning.

I think I could address some of the issues as we go along. Obviously, if your Honor has questions I could go to different parts.

What I tried to do is graphically represent some of the issues in the brief, and condense those down into a slide or two for each issue. If that is okay with your Honor, may I approach the courtroom deputy with copies of the deck.

THE COURT: Please. Approach Mr. Selecky, if you have a copy for my law clerks as well as, I don't know as well as for Ms. Johnson.

MR. ASSAF: Yes, your Honor.

May I approach?

THE COURT: Great.

MR. ASSAF: May it please the Court, this was the overview I actually prepared in anticipation of the Court's questions which I think actually tracks some of the Court's questions. So I will jump right to the issues, and as the Court once framed it, does the FTC have a statutory authority under Section 5 to regulate data security.

Before I get there, your Honor, I would like to take a few minutes to level the table and put it in context, this is the parties and the issue and then I will get into the statutory analysis issue.

So the factual background. Obviously on one side is the FTC, and I think it is very important to start off here. This is not, not some anti government plot. I have the greatest respect for the FTC, the historical missions, the results for the consumers. This is a fair minded discussion of whether, what they do under their consumer protection actions for consumers extends to data security.

So that is the FTC on one side.

On the other side is obviously Wyndham hotels. And one of the things that we are going to hear today, both in terms of the pleadings issues, and the statutory issues and the fair notice issue, is one of the key things here that I will keep coming back to is that the allegation is that that these Wyndham branded hotels, you have Wyndham in Parsippany, but then there are Wyndham-branded hotels, they own a whole series of franchises, Ramada, Howard Johnson, Wyndham.

And what the FTC, the crux of their allegation, is that cyber criminals use certain techniques to access personal information on the Wyndham branded hotels property management server. So let's just step back how, I got into this, I said oh, they are hacking into Wyndham.

Clearly, as you will see, they did hack into Wyndham's computer servers, but the credit card information we are talking about was actually stored on the local hotels server, the franchisees, if you will. So that is why we are going go to get into the issue of how far the authority goes for the FTC to regulate not only the company here in Parsippany, but then franchisees who are storing credit card information at their individually owned hotels all over the country.

The third set of parties here is Amici. I think there are a couple of points I would like to emphasize at the outset here.

First of all, as the Court I am sure has observed, it is unusual for the amicus to come in at the District Court level. This is the first Article III Court to weigh in on this issue and it has obviously much interest. The two entities I would like to call out here, your Honor, is the NFIB, small business group. 350,000 members averaging $500,000 in revenue a year in sales. And their average number of employees are ten.

And again, I would say it is significant that they decided to weigh in at the District Court because as we will see later in terms of fair notice issues,

and the FTC's argument on consent degrees decrease, a large number of consent decrees in the data security area are from small businesses.

As your Honor knows from your prior days on the bench as a magistrate, discovery costs are enormous, especially as you would imagine data security cases. So these people I think, they don't have a chance to contest this, a realistic chance to object. They have to enter a consent decree, because otherwise they will go out of business if they fight the FTC.

The second group is the International Franchising Association. 1300 franchisors, so if you are driving down the highway, it is, everybody. Tim Horton, Subway, whenever you see a franchise, most likely they are a member of this organization. Why do they have an interest, your Honor? Because that pleading that I showed you initially, can they be held for the Subway Sandwich Shop's protection of data security in Peoria, so that is why they are in.

Okay. Factual background. There is just the first slide, then we are going, we have one more and we will get into more of the background. These cyber attacks occurred in 2008. I think it is undisputed that they were perpetrated by Russian cyber criminals.

THE COURT: Let me ask a question. It happened in 2008. My understanding, at least, from trying to track it in the complaint, in about April of 2008, who was in charge of the data security at that time, 2008, April, 2008?

MR. ASSAF: Well, in terms of, a couple of answers to the question. Wyndham obviously is responsible for the data security at their corporate center. But as made clear on our website, including the very policy that the FTC refers to, the franchisees are responsible for their own maintenance of credit card information, which makes sense. You go into a Ramada in South Bend, Indiana, they swipe your card, they have your information. And yes, they have to communicate with Wyndham in Parsippany, but the crux of the allegation is that the South Bend, Indiana Ramada had the credit card information. So your Honor, clearly we are responsible for servers in Parsippany. Clearly.

THE COURT: That is what I am -- all right. You are admitting you are responsible for servers in Parsippany, but with respect to maintaining and keeping confidential this information you say it falls on the independently owned franchisee.

MR. ASSAF: Yes, your Honor. And to your, I

think your next question is preempted, is that it did start in 2008, and what happened is very sophisticated malware was used to crack into our system. I am going to show you in a second from down the hall, there is a criminal indictment, there are actually two of them here, which allege very similar facts which I will get to, Russian cyber criminals put malware on the system, in the back door like they did for us, and they came back later and used the back doors to gain entry to the system.

THE COURT: So in April, 2008, you would say the information was being held and the responsibility was being held by the independently owned franchisees, right.

MR. ASSAF: Yes, your Honor.

THE COURT: Then at some point counsel, though, I know, I told you I was going to interrupt you. At some point, doesn't Wyndham Worldwide Corporation takeover in terms of management of the information?

MR. ASSAF: Yes.

THE COURT: Counsel, I appreciate Power Point, and I am not in any way trying to give any one a hard time today, but the end result is, I can assure you I have read every brief. I have gone and looked

up every publicly available document even though you did not provide me, which I ask in the future both sides, if you cite to something, even if it is publicly available, I would ask that each of you take the time to at least provide me one courtesy copy of the document, and in particular, I am speaking of the, I believe, counsel, the way you pronounce it is CISPA.

You indicated in your brief, it is passed on 4/18/2013. My understanding, my research, correct me if I am wrong, I will get to that. You think it is sitting in committee and not currently law. But we will get to that. That wasn't provided, but I found it late last night late. My point is I will have questions for you.

I want to let you present what you are going to present. But I want to get to some of the heart and the meat of the questions that I have. So one of the questions is, at some point, at least FTC is saying that Worldwide Corporation took over some of the management of this information. And I wanted to hear you on that because you seem to be indicating that it really, all the information was in the hands during all of the breaches of these independently owned Wyndham hotels, or Wyndham-branded hotels. I

would like you to speak to that.

MR. ASSAF: Sure. In terms of Wyndham's response, they did undertake remedial measures. They hired forensic computer people to come in and try to figure out what was done, and in terms of responsibility issue that you are raising, your Honor, they notified the franchisees, they notified the card brands. They tried to implement systems for Wyndham.

But in terms of taking over responsibility for data security, they still did not take over, and I think that is a big legal issue, it goes back to why the franchisee association is here, is that franchisors at the end of the day cannot, in their view, and I am going to cite the Radisson case later on, should not be responsible for the computer systems of the franchisees. And how they maintain their data security, especially, your Honor, when it is prominent on our website that the franchisees maintain their own data-security system.

THE COURT: Okay.

MR. ASSAF: We responded to the investigation, notified the card brands, notify the Secret Service, and bring on forensic accountants, or forensic computer technicians. Of the FTC later on opened up an investigation, a million documents,

several witness interviews, at a cost of $5 million. They then file suit.

Now, since filing suit there are two issues that talk about the cyber security framework. There is cyber security litigation that is pending in 2012, you are right, never enacted and never signed. In response to that, President Obama issues an executive order asking for preliminary cybersecurity framework, and then fast forward to October 28 of this year, the federal government issues actually a preliminary framework of cybersecurity measures that are voluntary, to be sure, not the measure of law, an executive order, but that we will get to later on that we think provide important guideposts as to what companies should and should not do going forward, and so now at least those companies, arguably, will have notice of what is required of them.

And I will just note here, your Honor, that while those guidelines apply to banks, financial institutions, nuclear power plants, we would still comply with those guidelines as of today. So that is part of the anomaly I would suggest is part of this case, is that the federal government has now issued proposed, not regulations but guidelines, and we are in compliance with them.

THE COURT: But getting, let's talk about whether the FTC, let's cut to the chase, whether the FTC has this authority.

A lot of your arguments focus around Brown and Williamson, and the problem I am having and perhaps maybe you can tell me why this case you feel is so on point because when I read it, I really think it is distinguishable. And the reason I think it is distinguishable is because we have a situation where, as the Court said, since 1965 Congress has enacted six separate statutes addressing the problem of tobacco use and human health. We don't have that situation here.

What we have here is we do have something that is rapidly evolving, and I give you that, in terms of the concerns that the government has as well as the sophistication of these criminals and these hackers.

So yes, we have a situation where it is rapidly evolving, but we don't have Congress speaking to removing any, or extinguishing any power that the FTC has. And I read again CISPA, and there is no mention of whether the FTC has the authority or not. And quite frankly, where and how do you feel that this case, this Brown and Williamson case is as instructive

as you say it is?

MR. ASSAF: Okay. Let me go to slide 23.

Your Honor, the first argument is the argument about disclaiming authority. Let me address your question as to the other statutory --

THE COURT: We will get to disclaiming. I have questions.

MR. ASSAF: Let me address your issue on statutory -- on cases. That is I start with what I think you have been quoting, Brown and Williamson. This is important, I will go through the statute. It is a two-part answer.

First the law. At the time the statute is enacted, it may have a range of plausible meanings. Over time, however, subsequent acts can shape or focus those meanings. This is particularly where the scope, as here, I would argue, is fairly broad. And subsequent statutes provide more specifically address the topic.

So I would say to your question is there actually have been subsequent, there are numerous statutes since the age of data security. They are cited in our brief. The Fair Credit Reporting Act, Graham-Leach-Bliley Act, Children's On Line Protection Act, to start off. Why is that important? That is

important because it, because Congress, when they enacted that they said, for example, under Children's on Line Privacy Protection Act that the FTC were to issue certain regulations regarding data security. If the FTC already had that power there would be no reason for Congress to give them additional powers there.

So it ties in to what, to why I say the disclaimer issue is also important is that the FTC in the early 2000s recognized they don't have authority to regulate data security.

THE COURT: You know what? And I apologize. Go back to that. I do have some questions regarding the disclaimer here. Then we will go back to this issue.

Quite frankly, I am looking for case law that really supports your position that because the FTC has sought additional data-security legislation. It necessarily then lacks the authority under Section 5. And we will get to that question. Let me let you go back to this issue of whether they disclaim authority in early 2000. Tell me why you think they did.

MR. ASSAF: Okay. I start on with the Brown and Williamson statement. I point out obviously the case is not only important because it is a Supreme

Court case, I think it is more important because Judge O'Connor --

THE COURT: Let the record be clear. Whenever the Supreme Court says anything, it is incredibly important and I would of course defer to our Supreme Court. However, when I believe the case is distinguishable, I have to ask you why then the Court needs to consider it when I think it is perhaps clearly distinguishable. That being said, go ahead and state what you, what are you saying.

MR. ASSAF: Justice O'Connor I think lays out three possible ways in which an agency action would be seen as outside their authority. The first is disclaimer. The second is other statutes address it, and what I think it is shorthand for is is that when Congress acts in specific ways, it trumps a more general way or gives meaning to it, and the third issue would be especially an issue of rigorous public debate, it is hard to believe that Congress would have ceded this debate to an agency when the statute is either silent or ambiguous.

Let me address the first on disclaimer. In 1998 Chairman Pitofsky at the FTC was testifying on, this shows you how quickly things have developed, the worldwide web. And so I think the FTC was struggling

as to what their authority was under the worldwide web, both on the privacy side, and on the security side.

And here, if you look at what Chairman Pitofsky says, two things in his prepared remarks. He is trying to ask about whether businesses will self regulate or whether the FTC should be given authority to regulate businesses. And his view is, as expressed to Congress, that the FTC should get that authority because it is unclear whether businesses will actually self regulate, and he turns out obviously to be right. Businesses aren't going to self regulate.

What he says is that the Commission believed that unless the industry can demonstrate that it has developed and implemented broad-based and effective self regulatory promise by the end of the year, additional governmental authority in this area would be appropriate and necessary.

Footnote, important footnote: Currently the Commission has limited authority to prevent abusive practices in this area. The Act grants the Commission authority to seek relief for violation of the Act's prohibitions on unfair and deceptive practices affecting commerce, an authority limited in this context to ensuring that websites follow their stated

information practices.

So your Honor, I would argue the first time the FTC grapples with it, they say are authorities are limited here to if a company says something on their website, they have to abide by it. They are not talking here about the FTC determining what data-security practices companies should adopt. So this is the first step.

That same testimony, your Honor, the FTC says, gee, this is geared more towards privacy than security. And I would suggest that is actually not correct. It was not limited to on line privacy. In fact, if you look, this is for the record slide 19.

This is the conclusion in which he is asking for legislative authority from Congress, and again, the level said this, Justice O'Connor said you weren't asked for authority, you already have it. He says consumers are deeply concerned about the privacy and security of their own, and their children's personal information in the on line environment and are looking for greater protection.

And he then says, the four basic information practices required by the statute would be. So this is proposed. Would be. And then four is security integrity. Websites would be required to take

reasonable steps to protect the security integrity of that information.

So at least the first step, your Honor, not dispositive. So 1998, I would argue there is at least a step towards acknowledging.

THE COURT: But in 2000, and again, the Commission has argued, the SEC has argued that they began, and there are a number of these consent decrees, and they have said in their arguments that they have brought more than 40 data-security cases, 19 of which allege unfair practices, and have routinely reported a publicized data-security program.

The end result, counsel, that I would ask you is this at some point in early 2000 they began bringing these actions, quite frankly, you know, I think Congress would presumably have notice of these actions, since they have been occurring in over 40, actually over 40 data-security cases, 19 of which, again, alleged unfair practices.

Well, if there was a shift, I am not necessarily saying there was a shift in position with respect to whether they possessed the authority or not, they began in 2000 certainly pursuing these actions, and regulating and indeed enforcing when necessary. So you say what to that?

MR. ASSAF: Great question. I totally agree they started this roughly 2003, 2004. I have -- there are cases cited in our brief, consent decrees cannot form agency action interpretive guidance. It is how I started off, your Honor.

When you go again against, this is one of the names, Bonzai Auto Sales, that company is going to agree to a consent decree no matter what. One, we have great law that consent decrees are not litigated cases and don't form interpretive guidance. There is also the practical matter that there is no, in terms of consent decrees, we never have the information of investigations that don't end in consent decrees. That would also arguably provide some guideposts as to what is permitted and what is not permitted.

But more importantly, your Honor, this is right on all fours with Brown and Williamson, when the FDA starts to regulate tobacco, Congress obviously knew that. Congress didn't take action then to circumscribe that authority. There were lots of complaints in Congress about it. But the proper process is that in order to an Article III Judge decides whether the agency has authority. So the fact that the FTC, like the FDA, starts regulating something, and Congress doesn't do anything in the

first instance, doesn't surprise me because it is an exactly what happened in Brown and Williamson. Congress didn't do anything. Instead, an Article III Judge said, you know what, we get to look at that and decide whether the agency is acting properly.

THE COURT: So your point about the consent decree, though, wasn't TJ Maxx one of the entities that entered into a consent decree with the FTC?

MR. ASSAF: Absolutely.

THE COURT: That is a pretty big company you would argue, right?

MR. ASSAF: In term of that policy issue, let me address that straight on. You have company companies. TJ Maxx. BJ's, who have entered into consent decrease and it is not going to come as any surprise to your Honor, is that there is of course a path of least resistance, even though some of the consent decrees require a monitor for 20 years, that at some point, as we see from the record, companies large and small say you know what? It is just not worth it to fight with the FTC.

THE COURT: All right. I was countering your point about it being a mom-and-pop type of thing. We are dealing with some pretty sophisticated companies and they did enter into consent decrease. In

fairness, I think they would have also have resources to litigate, if necessary.

But that being said, let's move on.

Continue, counsel.

MR. ASSAF: Back to the 21. Chairman Pitofsky in 1998, and then in 2000 the Commission publishes a position on the dissemination of certain information. And it is clearly in the context of the FCC Act and in the context of COPPA, the Child on Line Privacy Protection Act. I quote from 21. The Commission's authority over the collection and dissemination of personal data collected on line from Section 5 of the act, and from COPPA, Which governs the collection of information from children under the age of 13.

Importantly at the end, as a general matter, however, the Commission lacks authority to require a firm to adopt information, practice, policies or to abide by the fair information practice principles on their websites or portions of their websites not directed to children.

I marry that, your Honor, that that is not just Wyndham saying, oh, that must help us. I marry that to the side panel to academic commentary on this very proposition from Michael Scott and the

Administrative Law Review. In its 2000 report the Commission indicated that while it had power under Section 5 to pursue deceptive practices, such as the website's failure to abide by its stated privacy policy, it could not require companies to adopt privacy policies in the first place.

And then 2001. Lee Peeler, who is the associate director of advertising practices at the FTC, in response to some issues with Amazon, and it is also important to understand, as I talk about this slide, the FDA was an issue over 60 years because of tobacco. I think we could all recognize, though, that obviously the digital age is moving much more quickly, so the timeframe here is compressed, but I would say in 2001, again, the FTC is going on record saying our authority is about deceptive practices. Deceptive practices. This is before any of the consent decrees that you referenced earlier in your questions or that are part of the record.

So I would say, this is the graphic on the next page, that from 2000, from 1998 to 2001, there are several statements, and then things clearly happen rapidly, your Honor. There are a number of consent decrees after that. But on the disclaimer point, I submit that Wyndham has a very strong argument that

the FTC, at minimum, was conceding that their only jurisdiction was over deception and whether your website was deceptive in terms of what you are doing for information policy.

Nobody from the FTC, prior to these consent decrees, were talking about the fact, and this is important, an important point, I have shown you actual disclaimers, but I would actually turn it around as well. Where is there any where from 1998 to 2001 where the FTC is telling Congress or even the Executive Branch, that we have this authority, so there is no need to do anything?

There is nowhere. So I have at least three instances. I would submit the FTC actually doesn't have anything where they go to Congress and in 2000 say we have this authority. There is nothing you need to do.

THE COURT: Okay. Counsel, I am going to shift gears. I want to hear from the FTC on this issue. Counsel does point to three separate instances where it appears at least that there is a question of whether you have authority. And I would like to hear your position only on that point. Then we will move back to counsel's additional points with respect to this issue.

MR. MORIARTY: Your Honor, Kevin Moriarty on behalf the FTC.

As I understand it, you only want me to talk about the disclaimer issue?

THE COURT: I want to hear what you say in response to the issue that in 1998 there was apparently at least statements on the record indicating that you did not have the authority to do what you are doing right now. And you would say what, sir?

MR. MORIARTY: As a preliminary matter I would say this case is very different than Brown and Williamson. I would say you understated how unique Brown and Williamson was. What the Supreme Court held was that the FDA's assertion of authority would require the FDA to actually illegalize tobacco products. And so the conflict between the FDA's position there and this 35 years of regulation was unique, and not anything like the conflict we are talking about here.

But just to limit it to the disclaimer, you know, I think all those reports and testimony to Congress, they really speak for themselves, and so there is not much use in trying to reframe them or argue about what they mean. They are all about, in

context, they are about this question that was coming up in the late nineties and the early two thousands which is that people were suddenly discovering that companies on line were capable of collecting enormous amounts of information about consumers, and people were suddenly realizing this. They are saying what are we go to go do about this?

And The FTC's position was, well, to the extent that we can't articulate an injury as a result of this collection, the companies are just collecting this information, and consumers aren't injured, then all we can do is prevent companies from lying or deceiving consumers about what their collection practices are. And so implicit in all of these is look, if consumers are injured, then of course we have jurisdiction because unfairness applies when consumers suffer substantial injury.

So that is sort of, that is the ground work of all these cases.

And you know, I can point out different spots in each of these cases where, or each of these reports or testimony where that is clear. You know, where we are limited in our authority to deceptive and unfair practices. But that is throughout these cases. And essentially the question that is being answered in

these supposed disclaimers is okay, well, consumers aren't injured, is there anything you can do about it? And the answer is well, if they are not injured, no, we can only stop companies from receiving it --

THE COURT: So you are saying it is a consistent position.

MR. MORIARTY: It is consistent. The other issue which again sort of gets into the weeds of Brown and Williamson, which I think is hardly worthwhile. I think Brown and Williamson is such an unusual case.

The other issue here is in Brown and Williamson, what happened was the FDA denied it had authority. Very clear disclaimer for 70 years. As a result of that denial this regulatory regime built up. But the earliest alleged disclaimer that they can identify from the FTC is 1998 or 2001. These data-security statutes that they are pointing to which again don't conflict in any way with the FTC Act, in the case of the FCRA, it was passed in the early seventies, maybe 1970, so there is no way that Congress was reacting to our disclaimer by passing that law. So really the disclaimers I think are a red herring.

THE COURT: Okay. Thank you, counsel.

MR. MORIARTY: Sure. Thank you.

MR. ASSAF: So addressing point one of the disclaimer, again, I think the FTC is saying that there is nothing -- there is no affirmative evidence, I think their position is that it must have existed all along. There is nothing in this record, your Honor, which they point to saying we have unfair jurisdiction and authority to regulate data security under the unfairness prong.

I don't, again, if I am wrong I will be corrected, but I think there is nothing in this record. So that is step 1 of Brown and Williamson, or at least one possible way that Brown and Williamson would apply.

The second one is what you and I started to talk about, the second prong. You don't have to prove any one of the prongs, but they are all instructive, to be sure.

And the second prong is whether there is other legislation that fills out the void and puts me meat on the bones as to what Congress meant. I actually think these are three, not only pre statutes, but three regulatory schemes that confirm that the FTC did not have unfair authority to regulate data security, and I am going to tell you why.

Let's take Bliley, 1999, right in the sweet

spot of the chronology. It mandates data-security requirements for financial institutions and instructs the FTC to establish standards for those financial institutions to protect against unauthorized access or use of customer records or information.

And what is so important about this, your Honor, I hate to preview fair notice, but there is some spillover, obviously. The FTC then issues regulations saying what data-security practices should apply under the statute.

Secondly, the Children's on Line Privacy Protection Act, 1998. Same thing. Directs the FTC to promulgate regulations requiring website operators to, quote, establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

And your Honor, let me address one issue. If the FTC is right on how broad Section 5 is of the FTC Act, there is certainly not an exemption for children under the FTC Act and whether it protects children's data security. So why would Congress, in 1999, seek then to create a regime for the FTC to not only have authority to regulate data security but it actually then tells them, which gets to our fair notice point later on, and they do this, issue regulations

protecting that data security.

And then finally, the Fair Credit Reporting Act, yes, although it was passed in the 1970's, to be sure, it was amended again in the sweet spot of this debate as we would describe it in 2003, that again, you impose requirements for the collection, disclosure and disposal of data collected by consumer reporting agencies and require the FTC and other agencies to develop rules for data handling in order to curb identity theft.

And the FTC then issues regulations on this, on data security.

So under the second prong or the second test for Brown and Williamson of whether there is other statutes out there that give guidance as to whether Congress has already given them this authority, I would argue there are at least three instances in which Congress then, in the sweet spot of this chronology, acts to give the FTC data security authority, and does so, and also tells them to issue regulations.

These cases are cited in our brief. I think, I respectfully disagree that -- Brown and Williamson is not only obviously authority, but it is, it also provides an analytical framework that other courts

have used in terms of what an agency tries to do something other than it is authorized to do. I don't think it is that unusual, it is not a one-off case. You have cases from the EPA, under the controlled substances Act, the FCC has been challenged. All on whether other statutes have made it clear that a broad statute is actually more narrow than the agency has said.

This is kind of a footnote to Brown and Williamson, your Honor, then I will get to the third point. I don't know where this comes up. I think it is in the FTC's brief in this section so I will put it here. The FTC I think also drops a footnote saying, well, no matter what, we get deference to determine our own jurisdiction, and they cite to the U.S. Supreme Court case, City of Arlington, Texas vs. FTC from this summer.

Well, your Honor, in Arlington, importantly, Arlington cites Mead, U.S. versus Mead, and it is an eight to one decision by Justice Souter. Here is what Arlington says about Mead. Mead denied Chevron reference to action by agency, with that rule-making authority, that was not rule making. I said there is spillover from the rule making and the authority. The FTC by the way for the first time ever, we briefed

this in Arizona and here, there is one line in their brief, we get deference to determine our own jurisdiction.

That only applies, your Honor, if they in fact have issued rules and engaged in rule making as to their jurisdiction. So I just wanted to pick this up, I didn't want to leave it there.

Now, I will get to the third point of Brown and Williamson, and that is, I will try to tie it all together, and address whether there is a limiting principle here.

Okay. The third point, Justice O'Connor says, there is disclaimer, there are other statutes. Then she says we must be guided to a degree by common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude to an administrative agency. We are confident that Congress could not have intended to delegate a decision of such economic and political significance in so cryptic a fashion.

That may be, that is the explanation point here. Because what we know from the record, and I am sorry your Honor had to go find the bills. There is charitably described a very healthy and rigorous debate between Congress and its interest groups and

the Executive Branch as to data security and how it should be done. That is going on right now. And so I would say Justice O'Connor's words only confirm under Brown and Williamson that there can be no argument that Congress, having now dealt with cybersecurity legislation and trying to figure out what it means, has delegated that to the FTC, and in fact, your Honor, I read the 2012 debates, and the 2013 debates, there is no serious notion the FTC is going to run data security for U.S. businesses.

The whole question is Homeland Security, and what Homeland Security is going to do in connection with the National Institute For Standards and Technology. And you would expect that. They have all the standards, and, why would Homeland Security be --

THE COURT: I also circled the section with respect to common sense because the only problem I am having is that if this is, if indeed Congress never meant to give the authority to the FTC and they know that, and it is clear, I have a hard time thinking that based on the security breaches and based on what we are talking about in this case, that Congress would not have acted years ago, and I understand the Court can't read into Congress's inaction or silence. But is the answer to not regulate? Is the answer to not

allow them -- they are again protecting consumers. And it just seems strange to me that if that was so clear, that Congress never intended to give them the authority, then we would not have seen some form of regulation, and instead what we are seeing is things are sitting right now and I understand this country is where it is right now, economically and the crisis that we all are faced with, various issues that face this nation at the moment.

But the end result is to say that Congress didn't intend to give them the authority and yet there has been nothing done, and in fact, we have, as you noted, there is, they refuse to they refused to act in 2012. So does that make, when we talk about common sense, does that make any sense?

MR. ASSAF: An excellent question right at the key point of obviously the third point of Justice O'Connor's analysis, that it actually I think cuts the other way in that while cybersecurity is clearly a problem, your Honor, the notion that the FTC is regulated through this litigated case against Wyndham when there are hundreds of data security breaches a year, and that there are no guidelines as the safe harbors, I appreciate that is a significant problem.

But there are also resources that address it.

There is obviously the criminal aspects, to go after cyber criminals. There are state Attorney Generals who are very active in this area in terms of consumer protection. They all have consumer bureaus that are very active in this area.

Unfortunately, there is a debate about this, too, but it is clearly out there. We know it from Reilly in the Third Circuit and Hannifer, there is equivalent of private Attorney Generals or private plaintiffs that if there is real injury that satisfies Article III injury, they also bring claims for data security.

So I would actually argue this is the worst of all worlds, because you have agencies, Homeland Security, criminals, state Attorney Generals, private parties, going after it. And here you have the FTC, who has refused to issue any regulations or rules or safe harbor provision as to what actually is required.

So your Honor, taking your premise that it is a significant problem, if it is a significant problem, I would argue then the FTC, or some agency of the federal government, should articulate exactly what companies should do for safe harbor provision, which gets into fair notice, I know, but that is the, that is to come -- that is, I think, the common sense

issue.

THE COURT: But what would you say to the SEC's position, we issued guidelines, protecting personal information and guides for businesses. We also have issued consent decrees, we are trickling into fair notice, but I think they really do overlap in many ways. I mean, they haven't necessarily, they would say, sat silently, have they?

MR. ASSAF: On two points, on the guidelines which I think, they cite for the first time these guidelines, I went and looked on the website, and they are just that. I mean, we will go through them on the Elmo, but they are the most vague and ambiguous guidelines. You should take reasonable measures to protect. They are a truism. And something that in law school we would say wait a second, you can't hold somebody liable for telling them, here are the guidelines, you have to act reasonably and we later determine what is reasonable.

I actually think the guidelines undercut their position.

In terms of consent degree, we will get into this, but the law is very clear the consent degree is not agency enforcement action that provides action to aggrieved parties. You saw this, for example, in the

FCC. The FCC consent decree, later on the parties agree, they can't then be held liable because another network entered into a consent decree that wasn't litigated.

But your Honor I think is getting at a point that I think bothers everybody, this is how I started off, is that how -- the FTC has an important mission here. Consumers are out there, and the FTC is trying to protect consumers, to be sure. How do you reconcile this?

I actually think, your Honor, that when you look at it that way, as to the FTC's mission, what they have done prior to this, and why I think it shows that this case is outside that authority, is that they -- under the unfairness and deceptive policy provisions, they have gone after fraudsters, phishers, schemers. Unscrupulous people. You just look at the Bureau of Protection website.

I couldn't find a single situation in which a third party who is the victim of a criminal attack, and we know that, I think you could take judicial notice of that given the indictment here. We have Russian cyber criminals. They are not going to dispute it.

You have a third party who then becomes the

focus of the FTC's consumer protection bureau. I think the way you reconcile all these cases is, it goes back to my limited experience with criminal law, kind of a malum in se issue. Are you engaged, are you as an actor engaged in a malum in se issue. I think it has basis in the case law. All of the cases we talk about, with the exception of this one, the data security group of cases, they are limited to malum in se things, where the actor is doing something they know is just wrong.

You go back to the primary purpose of Section 5 is to lessen the harsh effects of caveat emptor or the DC Circuit. They talk about what exactly the primary categories are: withholding material information; making unsubstantiated advertising claims; using high pressure techniques; depriving consumers of various post purchase remedies.

I have no quarrel, your Honor, that data security is a very important issue. I suspect the government, including the Homeland Security and President Obama's White House are trying to do something about it. My quarrel is that the FTC actually isn't the agency that is supposed to be doing it. They are supposed to be, and I would make the argument as a policy matter that the resources of this

agency historically and brilliantly have been used to protect consumers from scammers, thieves, and deceivers.

And to actually now go into an area which they have no real expertise, and I am going to get to that, your Honor. One of the issues in this case, your Honor, is hardware configurations, security networks. I know we are putting the cart before the horse, but we are accused of having unsecured hardware configurations or security standards that are lax.

Well, your Honor, we can show on the Elmo, we asked for discovery from the FTC as to what proper hardware configurations are. Forget that they haven't issued regulations for it. What they say is we object to answering that because the term "hardware configuration" is vague and ambiguous.

So your Honor, that is what I am saying. I can assure you, if I asked Homeland Security or the National Institute of Standards and Technology what hardware configurations are required for a proper network, I know now from President Obama's Executive Order, I know exactly what is required.

But the FTC, with all due respect, notwithstanding all the good they do for consumers, has no expertise in this area. So that is why I say

it comes back to the common sense point. I agree with you in the abstract. But let those agencies with the sophisticated technological expertise actually publish the guidelines.

I will get to that fair notice. So your Honor, I finish up on this point saying Brown and Williamson is not a one-off case, that Justice O'Connor writing for the Court laid out three ways in which an agency action can be challenged as beyond the statute's authority to that agency. We have shown you disclaimers and we have three or four of them, and they have none at the relevant timeframe saying this is our authority.

We have shown you subsequent statutes in the timeframe, under Brown and Williamson, that show that Congress knew how to give the FTC authority when they wanted to for data security.

Then we come to this point which I think is an important point, and that is, I would say it is not consistent with common sense to think that Congress in this environment, both good and bad, your Honor. I will finish off with this. Congress couldn't do it. I personally was disappointed in 2012 when they didn't get the cybersecurity act, because I thought it would have helped us here in this case. But they did not do

it.

But the political process worked. President Obama issued an executive order. I am going to go through chapter and verse as to what that executive order requires certain groups to do. It is going to become a standard that people can look at in the future. That is how it should be done.

THE COURT: But, and I am going to allow counsel to respond to the points made. But when we look at the executive order again, and when we look at CISPA, which again is pending legislation, there is nothing in there, or is there, that says that the FTC lacks authority?

MR. ASSAF: And we had a debate about this in the briefs. I know your Honor is getting to that point. There have been ten bills. Six of them had no savings clauses as to cybersecurity, which support us. They say but yeah, four of them had savings clauses. And none of those ten get enacted.

But again, the fact that we are having a debate that Congress six times doesn't put in a savings clause. Four times does. How could it be said that their statutory authority is clear at that point? I actually think that point cuts in our favor.

THE COURT: Okay. Thank you, counsel.

All right.

MR. ASSAF: Thank you, your Honor.

THE COURT: Now we will have counsel for the plaintiff address the Court. We sort of addressed disclaimer already. We have the issue of subsequent statutes and finally rounding off with the issue of common sense.

Counsel, I will hear you now.

MR. MORIARTY: Thank you, your Honor. So first I want to talk about the Brown case. The FTC Act is a consumer protection act. This FTC alleges that Wyndham engaged in practices that put consumers at risk, they deceived consumers as a result about these practices, and as a result consumers suffered substantial harm.

The substantial harm question is key here. The statutes that Wyndham is talking about, COPPA, GLB, the FCRA, they are all enactments by Congress that provide the FTC with additional tools to protect data security in certain circumstances. Specifically, when it comes to children's on line privacy, financial institutions treatment, and also information collections, companies' collection of consumers credit information in the context of the FCRA. What each of

these statutes does is say, either in the context of the FCRA they have specific rules are in the statute and in the context of COPPA and GLB, Congress stayed, requested the FTC issue regulation. But in all those cases what Congress did is say when someone violates the rule, when someone violates the statute, you can bring a case against them.

And so there is no injury requirement in those cases, so they are dramatically different than the FTC's authority under the FTC Act. Under the FTC Act we are limited to cases where we can prove substantial jury. We have alleged substantial injury here.

In those cases if someone collecting information about children on line, that is a violation. If a financial institution fails to have a written information security program that they update every year in response to likely threats to their information, that is a violation. Those are violations of those acts. In this case we have to prove substantial injury. So those cases are very different.

Of course, it bears repeating that this is a very different case than Brown and Williamson. In no way do those statutes in any way conflict with the FTC

Act.

And the proof is in the pudding here. The TFT isn't enforcing the FTC Act, the unfairness portion of the FTC Act, against companies for their data-security practices since 2005, and not a single conflict has arisen. Wyndham has identified a lot of the security laws, they appeal to this idea of common sense. I think we have addressed that, why those laws are different.

But you know, the key point of Brown and Williamson is there is a conflict here. The FDA's change in its position would have mooted those laws. It would have directly conflicted with those laws and as a result it was a Supreme Court's job to make both of those laws make sense since they both existed. That is why that happened that way. There is no conflict.

Wyndham has not identified a conflict, for the last almost decade we have enforced these cases, there has been no conflict.

Brown and Williamson is a very special case. I would point out the case law, Massachusetts versus EPA, I don't think it appeared in the briefs, essentially had exactly the same fact pattern here. The EPA said it couldn't regulate I believe CO 2 as a

pollutant under the Clean Air Act because at the time the Clean Air Act was passed Congress wasn't thinking about CO 2 as a pollutant. Then in later years other laws were passed, for example, against, required the Department of Transportation to have capped off standards for cars. The EPA was requested to start regulating standards for CO2 and they said no, we can't do it. Congress was not expecting it.

Second of all, there are other laws that couldn't plate regulation of this issue.

Third, it is a dramatic change in sort of the political and economic atmosphere for us to regulate that. And the Supreme Court said no. Those laws don't apply. Those don't conflict. Brown and Williamson applies where there is a clear conflict between the laws. That sort of addresses that issue.

I am just going to run through the points so this might be disjointed. Please ask me questions. As far as deference goes, the point of FTC versus Arlington is there is a distinction between a statutory interpretation and a jurisdictional interpretation of a statute by an agency. Our reference is whatever deference we should receive it doesn't matter that Wyndham is framing this as a jurisdictional question about the extent of the

authority or whether it was just a standard application of the FTC Act. It was not fully briefed, this deference issue.

I think is barely worth getting into it, and the reason is this idea of deference only comes up when the statute is not clear. In this context, we have a statute that prohibits unfair acts or practices in or affecting commerce.

THE COURT: You say clearly the statute is clear.

MR. MORIARTY: It is clear. The idea that the collection of payment information in exchange for services, the collection, the transfer, the maintenance of that payment information isn't a practice in or affecting commerce? It defies belief. It is squarely within the language of the statute. We don't have to get into the deference issue at all.

So I will move on to the idea that there are other statutes here and the stating of causes and the lack of stating of causes. As they pointed out in the reply brief, there is little point of trying to read tea leaves of Congressional inaction.

In addition, I would say in all those statutes, and in some of the statutes that they have identified, in some of the instances they have

identified the FTC going to Congress and asking for more authority, again this goes back to the COPPA and GLB issue, if there are regulations that said if, you have to take these steps or if there is a statutory law that says you have to take these steps regarding data security, we could enforce that law in the absence of consumer injury. That is not what is happening here.

THE COURT: The key is, in the absence of injury, you would not be able to enforce. Right? And so that --

MR. MORIARTY: Unfairness requires substantial injury, correct.

THE COURT: Right. So the reason that we have the FCRA and COPPA is because now Congress has said if there is a violation, you now have the authority to act.

MR. MORIARTY: Right.

THE COURT: That is why you believe those statutes are distinguishable from this case, and in this case, you clearly, you argue there is substantial injury, and therefore, you always had the authority to act.

MR. MORIARTY: That's right, your Honor. I wouldn't, you know, I would also point out that the

fact is that under Brown and Williamson there is just, there is core issues that are missing here. There is no indication that those laws conflict with, there is no indication that those laws abrogated or applied to -- that there is some previous lack of authority in the cases.

I guess the last point I will make is that, I think the idea that the FTC lacks any sort of expertise.

First of all, the factual questions are completely inappropriate here. This is a motion to dismiss. The response is to the interrogatories I don't think should be relevant to the Court's consideration. The idea we lack expertise is contradicted expressly by these statutes that Congress has passed that provide the FTC with authority to issue regulations on data-security practices, to issue regulations on privacy, that is, that's FCRA, GLB and COPPA. I think this is a disconnect there.

I guess the one other point I would make is they sort of belittled the guidelines that we passed, and, the guidelines that we have issued, those, the guidelines are for small businesses and they are important guidelines for small businesses. A sophisticated company like Wyndham, if acting

reasonably, would probably require more than just a little booklet in order to know how they should be setting up their network when they are connecting all of these individual franchise hotels.

But even those guidelines, and I don't have the particular guideline in front of me, based on the allegations in our complaint, Wyndham wasn't even complying with those guidelines that they say are very rudimentary.

THE COURT: We are going to get into the guidelines in terms of fair notice. I have a question for you. In terms of the way it works with respect to getting information and guidance from the FTC as to whether, and I am a large company. Are there mechanisms for these companies to sort of seek advisory opinions from the FTC about the security system they have in place?

I am just wondering, and I recognize this is a motion to dismiss, but I was curious in reading the papers last night that, you know, I am not familiar with what a company can do to sort of get an advisory opinion from the FTC as to whether their firewalls are adequate, as to whether indeed their data is centralized and protected. What is the process, just for my own edification?

MR. MORIARTY: We are pretty squarely within the fair notices category there. I think there are a lot of answers to that question, the principal one being that Wyndham in its privacy policy tells the consumers that they are going to take commercially reasonable steps to adequately protect their data. So you know, it is an objective standard, reasonableness, and for them to claim that it is now kind of a meaningless standard, it sort of rings hollow.

But as far as advisory opinions, there are not advisory opinions. But the way companies determine what is reasonable and what is not reasonable is the same way companies Act in any other legal context. The entire foundation of the common law negligence is requiring companies to Act reasonably under the circumstances. For example, in the context of data privacy they should evaluate the size and complexity of their network, evaluate the type of consumer data they are collecting and storing. They should evaluate industry standards. There are industry standards out there that are not associated with the FTC. There are experts out there that consult with companies routinely about the data security.

THE COURT: I am sorry to interrupt you,

counsel.

Does the FTC sort of endorse any particular industry standards that are out there? Are they published? How is that information disseminated in terms of what the industry standard should be?

MR. MORIARTY: Industry standards are well known. There are industry standards that specifically apply to the collection and transmission of credit card data. The FTC does not endorse any standards, particular standards. There is a Third Circuit case called Vogel which talked about whether a reasonableness standard should be pinned to industry standards. The Third Circuit said no, it should evaluate other reasonable things that companies in that position should look at.

The other thing I wanted to mention about FTC guidance is we have these books that we issue, guidance books. Also the adjudications are very valuable.

In this case in particular, I think it is that at page 19 of our brief, we identify a good number of the other, there is, at the time we wrote the brief, there were 19 unfairness cases. I think there is two more that are public. But we identified the particular types of things that companies should

be looking for in order to evaluate whether their data security is reasonable.

Now, we don't say here is how you should set up your router. We don't say you should have, you know, white lists and black lists for IP addresses. We are not tech support. We do say to them, companies, these are the types of things the FCC is looking at, you should make sure your house is in order on these things. The FTC provides guidance through these opinions, through these consent decrees.

THE COURT: Thank you. I will let you address any points you want to address after counsel argues with respect to whether the FTC has provided fair notice.

MR. MORIARTY: Thank you, your Honor.

THE COURT: Thank you. Mr. Assaf.

MR. ASSAF: May I have permission to make two reply points?

THE COURT: Sure.

MR. ASSAF: First of all, with respect to the FTC's point that Graham-Leach-Bliley, COPPA, that these were all cases in which Congress enacted them in order to avoid the FTC having to prove injury. That was kind of how they reconcile these cases. First of all, that is not in their brief. In fact, on page 12

they say something very different. I will get to the injury point. Page 12 they said they were enacted in order to give the agencies rule making, and/or civil penalty authority.

Now, I suspect they are running from the rule making authority, we are now paying into that. There is nothing in this record to suggest that those statutes were enacted simply to avoid the FTC or another agency having to prove injury. And how do we know that?

Because no statute can be enacted --

THE COURT: I don't know if that was counsel's argument, necessarily. I think counsel was saying that they, they cannot act unless there is substantial injury, and that this was Congress's way of saying if there are violations that necessarily are without substantial injury, just a violation, then they are -- they made it very clear to the FTC that they are free to act from that point.

MR. ASSAF: That point is not on page 12 of their brief. So I heard it differently. I heard injury. Because obviously, as your Honor knows, that Congress could enact a statute eliminating the injury requirement for Article III purposes, that is Reilly, they have to prove injury even if there is a

Congressional statute. A Congressional statute can't allow them in this Court without proving some sort of injury.

Secondly, your Honor, secondly, your Honor, the issue, this gets into fair notice, we are going to talk about advisory opinions. I think the answer to that question is not only are there no advisory opinions, but I want to put a point on this as we now get into fair notice, is that the FTC said well, companies should have experts, they should look at industry standards. The FTC doesn't endorse any industry standard, or tell you how to set up your router.

It is a great lead-in to fair notice, because now, if this litigation goes forward, you are going to hear the FTC at this podium complaining about bringing in an expert that says this router configuration is what should have been done, and what should be done by Wyndham going forward.

And so not only is there no advisory opinion, but there is actually, up until today, the FTC, even in their pamphlet, has never provided any discussion of what actually is required. We are going to get into that with fair notice. So let's talk about that.

THE COURT: Again, counsel, the purpose of, we are here on a motion to dismiss. And a lot of the arguments that we are going to get into, and I just, I am wondering whether these arguments aren't left for trial, in the sense that determining whether one security system is adequate and/or reasonable. Aren't these issues that, quite frankly, are best left for trial, and are they necessarily ones -- an issue that the Court needs to resolve in a motion to dismiss?

MR. ASSAF: Let me address that, your Honor. If there is a trial as to whether a company's security measures were adequate or reasonable, that is a separate question as to whether, today, or at the time of the filing of the complaint, a company had notice of what the FTC standards were. I actually just break that --

THE COURT: But isn't that more for a summary judgment? Isn't the argument that you are about to make, and I am going to let you make them, but aren't they best left for a dispositive motion? Once discovery has been had? Because what if indeed there is some evidence, and I am by no means saying there will be, but let's say there is some evidence that internally Wyndham knew that there were issues, that they were aware of what some of the industry standards

that they were concerned about some of the stuff that was coming out of the consent decrees, and that they were aware that their present security system was inadequate. Isn't that, in essence, isn't that helpful to know, and doesn't that have to actually, don't we have to let discovery play out before one can stand at a dispositive stage and say we didn't have adequate notice?

MR. ASSAF: I think that would turn fair notice cases on their heads. There would never be a fair notice case on the pleadings and they are all, as I see them, all these fair notice cases are on the pleadings, because otherwise you would have a company have to go through discovery in order to raise the fair notice question. The whole purpose of the fair notice doctrine is that prior to being hailed into court, and be subjected to an enforcement action, that you had fair notice of what the prohibited activity was.

THE COURT: But the cases you cite, weren't all of them summary judgment motions?

MR. ASSAF: I will check that when I sit down, your Honor.

THE COURT: They are. If they are not, correct me. I could have sworn they were all

dispositive motions. They weren't brought necessarily on an MTD stage.

MR. ASSAF: I will check that when I sit down. I suspect now. Let me start off with the FCC cases, these are not cases in which you need to develop a factual record as to what exactly the regulatory environment is, because you actually know on the pleadings.

And so could there be some summary judgment issues that the Court said I need more facts just for a limited issue to complete the record? I think so. But I don't think we are going to go through years of discovery and determine anything else in terms of the notice issue.

Because your question goes to two different issues: What notice were we on versus what our knowledge us. I suspect issue one as to what the notice is, that is done on the pleadings. So let's go through that.

FCC versus Fox. This is where we start off, Supreme Court 2012, fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden. GE versus EPA. In the absence of notice, for example, where the regulation is not sufficiently clear to warn

a party about what is expected of it, an agency may not deprive a party of property by imposing civil or criminal liability.

This, so this actually goes exactly to the point that not -- here I argue there is no dispute as to whether the regulation is sufficiently clear because I am going to get to the point that they haven't published any regulations. So this is actually the most extreme case of fair notice.

Most of the fair notice cases say, are these regulations sufficiently clear? Here, there is no dispute on this record. They are not going to dispute it, that there is no regulation. So that is what I think, your Honor, in terms of the cases, most cases come up to a court where there is actually a regulation in issue.

So we start with the Third Circuit, Dravos with an OSHRC regulation. The Third Circuit Said the agency must be able to state with ascertainably certainty what protections a company must employee in order to comply with the regulation. Here I would argue there is no as certainly regulation because there is no regulation. The FTC has not published any rule or regulation.

We already know, I previewed this in the last

section, your Honor, that Graham-Leach-Bliley, the Fair Credit Reporting Act, and COPPA, they have authority to publish rules. But under Section 57 (a) they also have the authority to prescribe rules and general statements of policy, and they have not done that for data security. There is no dispute about that.

This is where again it is not just Wyndham. I would suggest there is academic commentary saying the nature, format and content of the agency's data security related pronouncements raise equitable considerations that create serious due process concerns, what I call fair notice.

So what are the arguments?

Now, I understand, your Honor, I am going to get to the agency's arguments, and I understand that these are requests for admissions, but I think they actually filed them in this Court. And again, there is not any dispute here. The FTC has not published public information about what security software should be used by a company. Admitted.

And the FTC has not published any substantive rules or regulations pursuant to their statutory authority explaining what data security protections an individual or entity must employ to be in compliance.

So I want to marry that with the Dravos quote from the Third Circuit which said is an agency must explain with ascertainable certainty what must be employed.

Here, they can never meet Dravos because they have not published. What do they say? They say reasonable notices --

THE COURT: All of this sounds of summary judgment. You are asking me now to consider requests for admissions, things that are outside our pleadings here, counsel. We are here on MTD. That was one of the things I struggled for the last week is many of the arguments you are making to me sound like they are going to be appropriately made at a later juncture. But at an MTD hearing, I am having trouble understanding how the Court should be considering a request for admission at this point.

MR. ASSAF: So let me address that, your Honor. Put the request for admission off to the side. There is not going to be any dispute. The Court can certainly take judicial notice, there are no rules, regulations, or policy statements published by the FTC.

You can open CFR, you can go to the agency website. You can obviously take judicial notice of that. And they are not going to dispute it, your

Honor. It has been dispositive in their briefing. They said we haven't published rules and regulations. I am sorry on to use the RFAs, but I don't really need them. There is no dispute they haven't published them. On the summary judgment point the record is clear that there are no rules or regulations. What does the FTC argue? Instead of rules and regulations it should be reasonableness, reasonableness is the touchstone.

THE COURT: What about the best practices? Are you going to get me there? Because clearly the best practices, and the Court read them yesterday and counsel is saying when you look at the guide, that they submit he failed to follow even the very basic rules that were, or at least the very basic information that was provided by the FTC to businesses and small businesses in this particular informational paragraph.

MR. ASSAF: I am definitely going to get there. Let me preview it. First of all, I think I said, reasonable practices, because even their pamphlet just says reasonable practices. They don't say best practices.

So, I am going to get you there. There are three arguments the FTC says, or makes out. The first

is, rule making is not feasible here. That is their first argument.

The second is we have published these consent decrees and they should give you guidance. And the third is you can look at private standards or read what the industry or best practice -- reasonable practice is. And I have responses to all three that I think on a motion to dismiss are properly in front of the Court.

THE COURT: Okay.

MR. ASSAF: So first I start with the FTC brief on slide 46, that it would not be practicable for the FTC to establish through rule-making the highly particularized guidelines that we suggested should be published.

Now, I would suggest, your Honor, again, you can do it on a motion to dismiss. We know that argument cannot be persuasive because the FTC has in fact published particularized guidelines under Graham-Leach-Bliley and under COPPA. And even again, this is a matter of public record in the CFR, they published very detailed guidelines in the Bureau of Consumer Protection of what it means if a company hit green. And so I would argue that if the FTC Bureau of Consumer Protection can publish regulations on data

security for Graham-Leach-Bliley and COPPA, and they can publish detailed regulations on what it means to be green, they can at least publish some regulation here. I don't think it is not feasible to publish regulations.

In addition, as your Honor knows from doing your own research on the Cybersecurity Act and the Executive Order, and again the Court can take judicial notice of the Executive Order by the president, that is done, that is part of the record here, is that the cybersecurity framework lays out in detail certain protocols that they encourage companies to follow. So this goes to the feasibility issue. If you have one executive agency publishing guidelines, and I am sorry they are so small but they are on the slide 51, very interesting, your Honor, if you look at the bold on the right, COBIT, BA, ISP, CCS, TEC.

These are all references to certain hardware and software protocols. So when we talk about fair notice, your Honor, if the FTC had done what the Department of Commerce and the Department of Homeland Security had done, and published certain guidelines, then this would be a far different argument.

And so why am I putting this up here? Because I think it completely cuts against the FTC's

position that it is not feasible to public guidelines as to what you should be doing. Two other executive agencies, the Department of Homeland Security and the Department of Commerce, have done it.

Now, the consent decrees. We talked about this in the first set of arguments, too, that the FTC responded that there are consent decrees. I think these, as I pointed out earlier, are only FTC victories. They are clearly not binding on the FTC. If I came into court and said that this consent decree was binding on the FTC as precedent, I do not think that that would fly under the law.

And they are still vague. And why do I say that they are not legally binding? If you turn to the next page, slide 53, is that court after court has said the entering of a consent decree is not a decision on the merits and does not therefore adjudicate the legality of any action by the party thereto, nor is a consent decree a controlling precedent for later Commission action.

Kenwit, on the Federal Trade Commission, courts and FTC have construed consent orders as contracts rather than as binding judicial precedent. The Federal Circuit, consent order does not establish illegal conduct. And so forth. I don't think there

is any Court of Appeals cases suggesting that consent decrees are binding or even persuasive, or even binding on the agencies, yesterday alone other parties.

And again, your Honor, this is just an idea of consent decree. This is a matter of public record, so I am cited on a motion to dismiss. These are the types of consent decrees, they go through some of the factual allegations, and they talk about, in large part, of remedies, the 20-year monitoring is what the company has to do going forward.

Then finally, your Honor, on the point we started your question about private or industry standards. So the FTC says private standards provide fair notice. Or industry standards, or reasonable standard. I could be corrected, but nowhere has the agency ever said that in terms of rules, regulations, or policy guidance.

They said we encourage you to undertake reasonable effort, but they never said your reasonable efforts are the touchstone and provide you safe harbor. I still think that is ambiguous. But I don't think they have issued rules or regulations saying we are going to look for industry standards in order to provide you a safe harbor, which goes back again to

Dravos, that a company has to have some notice of what we can do to stay out of trouble.

The FTC, importantly, your Honor -- you asked the question, can you get an advisory opinion? Have you, the FTC, ever adopted industry standard? Importantly, your Honor, they have the ability to do that, and in fact, the SEC, again, a matter of public record, they have adopted FASB, an accounting standards board. Look to FASB. That is what the FTC can look to as the private standard. The FTC can say we will adopt the standards adopted by the Commerce Department, by Homeland Security or by private standard, but they have not done so.

So your Honor, that is where I think the cart before the horse issue, that they have to tell me in advance what my improper conduct is, and importantly, consistent with Dravos in the Third Circuit, forget about the ascertainable certainty. I don't think there is any real debate there is no ascertainable certainty here. But importantly, for the Third Circuit purposes, what can I do as a company in order to make sure I am in a safe harbor?

And even as of today, no company can get up here, FTC can file against any of the hundreds of companies who had a data breach by alleging you have

unreasonable security practices. We are in court, I will make this argument. The FTC he will never ever worry about a motion to dismiss under their view. All they have to say is we alleged unreasonable security practices. Let's go forward with discovery. That is all they have to allege, no matter what the violation is.

So your Honor, I have no way, as a defendant, to know what I need to do to stay out of the FTC's aim, or more importantly what I can do in front of an Article III Judge to say, here re the regulations with ascertainable certainty, and my client abided by those regulations. Right now, I can't do either. And I think that is inconsistent with the Third Circuit law. Then we get to deception.

So I am happy to answer any questions, your Honor, but that is the outline of my argument. Again, I don't think there is going to be any dispute that there are rules or regulations, there are none out there.

Thank you, your Honor.

THE COURT: Okay. I will hear from counsel for the FTC.

Do you concede there are no rules and regulations that are currently available?

MR. MORIARTY: Regarding SEC Act liability, no, there aren't for data security. There are for GLB, which counsel pointed out. Graham-Leach-Bliley regulations were issued by the SEC, which goes back to the expertise.

I actually would like to touch on the guidelines from GLB for just a second. Those are the guidelines that if a company violates those guidelines they can be held liable under the FTC Act without injury.

The guidelines, if you look at them, require companies, I mean there are several, I think there are four different steps, but sort of the linchpin of the guidelines is that companies must take steps that are reasonably designed to protect consumer data. And this idea that through the GLB guidelines the FTC has created very elaborate technological regimes where companies can know precisely how to protect their data is inaccurate.

Just to step back for a second, I think the basic premise of Wyndham's fair notice argument is that they don't know how to comply with the reasonableness standard when it comes to protecting consumer information. The argument is problematic. First Wyndham states in its privacy policy it is going

to take reasonable measures to protect consumer data, so they invoke the same standard that they now say they can't comply with because they don't know what it means.

My second point is that this is a standard that companies comply with all the time. I made this point before in a variety of contexts, in common law negligence, in competition law. And actually, in data security, in private data-security actions, negligence actions against companies, the Court, the parties, they evaluate whether the company acted reasonably with consumer data.

And in those cases, your Honor, the defendants are susceptible to a lot more liability than they are in FTC Act ways. We concede equitable relief in those cases, plaintiff can get damages. I guess my basic argument is they are proving too much to say that they don't know how to comply with the reasonableness standard because that is how a lot of the law works.

THE COURT: Which is the standard? Is it reasonableness or is it ascertainable certainty?

MR. MORIARTY: So I think their argument so our standard is reasonableness. And they argue that reasonableness does not provide parties with

ascertainable certainty.

As a side note, there is a Third Circuit case called Secretary of Labor versus Beverly HealthCare-Hillview, 541 F.3d, (2008).

THE COURT: 2008 case?

MR. MORIARTY: Yes, 2008 case, that states that ascertainable certainty is not the standard. I believe the conditions are that if agency hasn't reversed itself, and if the interpretation is publicly available, an ascertainable certainty is not the standard. We certainly satisfy that.

THE COURT: I was going to ask counsel, I actually was going to provide counsel with a copy of that case this morning. And I wanted to hear from both sides as to their opinion with respect to this 2008 case because in preparation for today's oral argument I came across it, and neither side had noted it in their briefs.

So you would say, though, that based on the Third Circuit's case in 2008, the Court does not necessarily have to apply the heightened standard.

MR. MORIARTY: I agree. But I dispute that the reasonableness standard does not provide companies with ascertainable certainty. And I think that is squarely within Third Circuit precedent. I think the

idea that reasonableness does not provide fair notice to companies has been foreclosed by the Vogel case. In that case, the Third Circuit held that an agency regulation predicated on enforcing a reasonableness standard did provide fair notice to regulated entities.

This case appears in our brief at page 20-30. That is a 1980 case.

So the last point is --

THE COURT: Let me understand your position. I am sorry, counsel, to make you go back.

Does this Court apply a reasonableness standard, or is this Court bound to apply, based on counsel's argument that the Dravos case, that the Court then must implement a heightened standard for enforcement? Or are you saying -- what exactly is the FTC's position?

MR. MORIARTY: The FTC's interpretation, well, as a preliminary matter the substantial injury, unfairness complication of substantial injury requires parties to balance benefits to consumers, it is basically substantial injury to injuries versus countervailing injuries. It is essentially a cost-benefit analysis.

In the context of data security, since 2005

in the BJ's complaint, the SEC has expressly said as applied to data security that unfair application requires companies to act reasonably with consumer data. Reasonable is just not word for the cost benefit analysis that reasonable parties should undertake.

So our argument is that ascertainable certainty does not apply because we have been consistent all this time. We have consistently said, essentially since the codification in 1994, and certainly since we brought our first unfair data security practices case in 2005, that reasonableness, the cost benefit analysis is the standard for data security practices, so as a result, the ascertainable certainty standard under Beverly Healthcare doesn't apply.

But I would further argue that reasonableness is an objective standard recognized under the law and does provide ascertainable certainty to companies.

So a separate issue which we have gotten into a lot is whether the FTC should fill out the precise contours of reasonableness by issuing rules and regulations, or whether to proceed by ad hoc adjudication. And this is squarely within the agency's informed discretion, this is the Chenery

case, and the NLRB vs. Bell Aerospace case especially where, as here, it is doubtful whether any generalized standard could be framed which would have more than marginal utility.

In the first FCC versus Fox, a Supreme Court case in 2009, the Supreme Court affirmed this approach of the FCC evaluating an obscenity, it said it could proceed on a case-by-case basis, and in fact this arose in the Vogel case in 1980 where the subsidiary argument of the defendants, after saying reasonableness didn't provide notice, they said at least they should have provided us with regulations or guidance to tell us what reasonableness means, and the Court said, this is just standard law at this point, quote, is within the secretary's discretion whether to proceed between ad hoc litigation and regulation.

So I just thought I might address some of the points that they raise. And in fact I forgot previously to address the point that they made in the Brown and Williamson section. I will make it short.

THE COURT: Sure. Counsel, I want to let both sides know, make all the points you feel necessary. I am not cutting any one off today.

MR. MORIARTY: The idea that FTC Act only

applies to parties that are engaged in fraud is just inaccurate. It is not based on the statute. Unfairness, the injury requirements, plainly don't have any limitations.

So getting to this case specifically, or getting into the fair notice issue. So BJ's is clear. I can -- that is a 2005 case, applying the unfairness case to data security. Respondent's failure to employ reasonable appropriate security measures to protect personal information caused or likely to cause substantial injury to consumers that is not offset by countervailing --

THE COURT: Slow down and start from the beginning, counsel.

MR. MORIARTY: I don't have to read it. The reasonableness standard satisfies the codification of unfairness, which is at 15 USC 45 (a). That is essentially what I was reading, is the statute.

I don't think it is of great value to cite academic articles in this case. I know that some of the authors of those articles are also practitioners. I don't know if that affects the Court's valuation of the value of their academic opinions. I am not saying that they are wrong or denigrating them in any way. But to say that they are, you know, dispassionate

observers is probably not accurate.

So one of the issues on rules that they raise is why doesn't the FTC issue rules, and the answer is that the FTC Act, unlike Graham-Leach-Bliley which applies to only financial institutions, the FTC Act applies to all companies engaged in commerce. In order to create a rule that apply to everyone equally, we might end up with a rule that is very onerous to small businesses.

In fact, your Honor, it is a position that the Chamber of Commerce frequently takes when it objects to statutes, that Congress is attempting to pass, as they say, look, Congress can't possibly substitute its judgment for the dynamic reasonableness assessment that small businesses take, nor can it create a rule which equally applies to everyone in a fair way.

So to the extent that the FTC tried to issue rules take are like frankly the cybersecurity guidelines, which are designed to protect critical infrastructure, that would be incredibly onerous to small businesses that aren't protecting dams, or the electric grid. So a reasonableness standard is far more fair to all companies that we regulate. And again, it is something that businesses do all the

time.

So the last point that I want to make is with these consent decrees, there are consent decrees and then there are also complaints. And the idea that they are not binding on this Court, we don't argue that they are binding on this Court. It is a red herring.

What we argued, the purpose of decrees is to provide parties with notice about the application of the FTC Act and about the types of things that the FTC evaluates when determining whether a company is engaged in reasonable practices with regards to consumer data.

THE COURT: So you say, counsel is arguing that they are not binding, and you never submitted that they are binding. But what you are saying, the real issue here is do these consent decrees provide notice to businesses as to what you need to be doing, and if you are not doing, there is danger.

And so you say that by -- counsel, I don't know whether it was in, it is probably in the reply brief, one of the things they say is all these consent decrees are very -- they are a case that deals directly with this particular company. And it is very difficult for us to say, well, based on those facts

are we in danger? And that they don't provide, you know, adequate warning or adequate notice as to what they need to be doing. And you would say what to that?

MR. MORIARTY: So the answer is that they do provide a lot of information, but we are not exclusively leaning on those adjudications, those consent decrees and complaints as the only source of fair notice. Nor would industry, I believe, accept it if the FTC stated we are the sole arbiter of what is reasonableness.

Reasonableness is an objective standard. It is not the FTC's reasonableness and Wyndham's reasonableness. Reasonableness is objective. There are a lot of sources companies can look to. There is no single answer. That is what happens all the time in the law.

So if a company is trying to figure out, if the grocery store is trying to avoid slip and fall accidents, the common law that they might look at won't be exactly their grocery store, you know, circumstances won't be the same, the type of threats to consumers might not be the same, but they can still make reasonable judgments based on previous cases and a variety of industry standards and just the general

circumstances of their particular instances. That is just, that is just how the common law works.

THE COURT: Can we talk a little bit about the best practices guidelines, and can you walk me through, perhaps, where you said earlier, even if you look at the very simplistic guidelines that counsel says are available, that there were violations you allege by Wyndham of the very basic rules?

MR. MORIARTY: So one of the key principles of the guidelines is data inventory and data management and data minimization. And the allegations in the complaint are that Wyndham permitted companies, or on the Wyndham network there were hotels with unencrypted information, and because of the lack of password policies this information wasn't segregated from anyone else who might also be able to get on the network. So that is kind of a basic flaw which we have alleged in paragraph 24 of our complaint.

And again, there is the guidelines but there is a lot of other stuff out there that would make a lot of these vulnerabilities that we have identified, they make them reasonably known to companies that are trying to practice data security.

THE COURT: Let's look at them, one of them electronic security, make it your business to

understand the vulnerabilities of the computer system and follow the advice of experts in the field, and identify the computers the servers were sent to the personal information is stored. Identify all connections to the computers where you store sensitive information. These may include, and you go on to say, internet, electronic cash registers, and so on. Encrypted, sensitive information that you send to the parties over public network.

So there seems to be at least some information here, and you say that some of this information wasn't publicized here.

MR. MORIARTY: That's right, your Honor. You articulated it much better than I was.

Yeah, I point to paragraph 24, we alleged failure, not of that guidance, but of the complaint, we alleged a failure to segment the network, we alleged a failure to encrypt data, we alleged a failure to change default passwords available on the internet, a failure to have password policies that require strong passwords. These are all things that, some of which might be mentioned expressly in the guidance, but are all things known in the industry as commonly known, and easily avoided vulnerabilities that a company that is acting reasonably to protect

consumer data could avoid.

THE COURT: Anything else, counsel?

MR. MORIARTY: No. Thank you, your Honor.

THE COURT: Let me check with my reporter.

We are going to take a break. Ten minutes. And then we will let counsel respond.

(Recess).

THE COURT: We are back on the record in FTC versus Wyndham, civil action 13-1887.

We took a break, and we are now ready to hear from counsel for Wyndham. During the break I provided counsel for Wyndham a copy of 2008 case that was cited by the FTC's counsel, Beverly Healthcare-Hillview.

MR. ASSAF: May it please the Court, I appreciate the copy of the case. It was not cited in our brief. I wish it had been. Actually, I think it supports beyond any doubt our position in the case. 2008 case Beverly Healthcare talked about Dravos and said Dravos doesn't apply when -- may I leave the podium, your Honor -- the agency had given conflicting public interpretation of the regulation. We are not arguing conflict, or the regulation at issue. The regulation is so vague that the ambiguity can only be resolved by deferring to the agency's own interpretation of the regulation, and the agency has

failed to provide a sufficient, publicly accessible statement of that interpretation before the conduct in question.

So a couple of points, your Honor. First of all, in this case the Secretary of the agency, or in the FTC case, the Commission, had actually published a regulation. So there is a regulation at issue that I would argue, I understand under Dravos, you then at least have a regulation for context.

After that,, your Honor, two things happen: One, the agency, or in this case, the Commission, issued two directives, publicly available, on the meaning of the regulation. Then what happened is that the agency, or the Commission, had two litigated, not consent decrees, two litigated cases explaining the regulation and the interpretation of the regulation.

So on one side you have post Dravos a situation where the agency issued a regulation. They issue a directive saying what the regulation means. They litigate cases under the regulation and the Third Circuit unsurprisingly says Dravos doesn't apply in that case.

Here, no regulation. And certainly no interpretations of the regulation because there is no regulation.

Counsel conceded when they stood up, your Honor, the very first thing they conceded, there are no rules or regulations here. And I haven't completed a full analysis, your Honor, of your question about, well, aren't these cases resolved on summary judgment? My initial analysis is that, for example, Dravos, Fox, GE, they are only not summary judgment.

THE COURT: They go right up to the Circuit. Counsel, we are in a different position right now. We are in a different position. They don't have a regulation that you are obviously taking right up to the Circuit. But in that instance, this is as you all are saying, as you know, a unique situation for this Court to be, and many of the arguments that you are making, I believe, and I am going to consider them, I haven't pre-judged this issue, but I think many of these arguments, at least as to notice, maybe not standing, what I am calling standing, the issue of whether the FTC has authority. That obviously I have to resolve at an MTD stage. I understand that.

But the issue of fair notice I think is an issue that, at least when it is dampening your argument, seems to at least require that some discovery be done as to what notice you were on as to what reasonable standards were, because there was a

policy statement which you said you were observing industry standards.

We have to understand what you understood those industry standards to be and whether indeed there was an issue of notice. You say not, and I understand you, that is what we are here for. But I quite frankly think when you look at those cases, we are in a different posture today than many of those cases when they went directly to the Circuit for guidance.

MR. ASSAF: Your Honor, this is such an important point.

I would like to try to convince you otherwise. I will start with the regulations which it is exactly opposite. You are saying, well, we are here because there is no direct appeal of the regulation. There is no direct appeal of the regulations because they have not published the regulations.

THE COURT: I understand the point.

MR. ASSAF: So your question, by the way, and I want to come back to the industry standard point, but your question was, well, there is an argument here that, well, we don't want to publish regulations because it might be unfair for small businesses. They

made that argument.

Under administrative law, your Honor, it is exactly the opposite. They don't get to stand up and say, we get to determine how to enforce the law without regulations based on our own decision-making without regulations. If they have a concern with how they impact small businesses, that is what administrative law is all about. That they need to publish the proposed regulation. Get comments and testimony on the proposed regulations. I guarantee you, like the cybersecurity act, that people will come in saying the way you phrased this would impact negatively on small business, and therefore, we suggest that you do the opposite.

They would have lots of comments, lots of testimony, and then we would have a regulation. But they don't get, with all due respect, they don't get to come up and say we are not doing a regulation because we think it would be hard for us to administer. That is the exact purpose of the administrative law and the whole promulgation of regulation process, is that they have to publish a regulation, they have to give people notice as to what the regulation means. Give us a chance to comment on the regulation, and then there due process is met,

because they will have considered the small business impact, et cetera.

THE COURT: So you are saying that there must be the publication of a regulation.

MR. ASSAF: There must be.

THE COURT: And without the publication of a regulation, there is no fair notice.

MR. ASSAF: There is no fair notice. I think under Dravos and the Supreme Court cases and it answers your question about why are we here? Because could we only do this on summary judgment? The reason we are here is because if they had a regulation, we could have either, A, challenged that directly to the Third Circuit --

THE COURT: Is there any case that says there must be a regulation in order for there to be fair notice?

MR. ASSAF: Well, I think there are cases in our brief. I will get it on my reply once I get them out. I think it is black letter law that an agency with rule-making authority, which they have, they have rule-making authority, Congress has given it to them, that when they are going to take action, enforcement actions, that they have to publish regulations in order to give companies fair notice of what is

prohibited by their actions.

And so, your Honor, your point, or your question as to, and I understand it, I was sitting there saying why are we here, why aren't we at the Third Circuit already?

And the reason is that if they had published even a one-page regulation, and they don't want to do it, they know we would take them to the Third Circuit in a heartbeat saying this is arbitrary and capricious, it doesn't give fair notice, et cetera, and the Third Circuit under Dravos would say no ascertainable certainty. Try again.

That is why the telling part of the argument is, it might impact small businesses differently, we don't want to publish the regulation. That is the precise part of the law and why Article III courts are so important, because you cannot allow an agency simply to say we get to decide in our own halls when they are going to enforce things and what we are going to enforce. Otherwise, by definition there is no notice.

I am sorry, I am animated on this one. Your question on why we are here, it got me thinking at the break, she is right. Why are we here? Why aren't we in the Third Circuit.

THE COURT: You want to skip right to the Third Circuit on me?

MR. ASSAF: Yes, wait. There is no regulation. There is no rule. And I read this case, and I said, exactly. This is, Judge Fisher is working with an agency, with the statute, that had a regulation that then had interpreted decisions under the regulation that litigated it, and litigated cases, not consent decrease, he says, you know what? The regulation, you know, isn't subject to a Dravos challenge.

If they had that regulation, we would be having a wholly different argument in front of three members of the U.S. Court of Appeals for the Third Circuit. But here, your Honor, it is not only the regulation is vague. There is no regulation, but again, it is the unfairness, by definition you need something.

THE COURT: And counsel, let me just say that quite frankly, a lot of the arguments that you forwarded in your brief and today on the record, these are arguments that I think are going to be available to you, not now, we are not talking about the authority issue, I am speaking directly to the issue of fair notice. These are arguments that, quite

frankly, the reason I said why are we doing this now is because I think that once there is discovery, then these arguments with respect to you not being on -- there not being fair notice, are going to come into play, and the FTC is going to have a job to do with saying that there is -- the notice is adequate, and the notice is reasonable, and whose standard are we utilizing.

All these seem to be arguments that are ripe for dispositive motions and not necessarily at a motion to dismiss.

But you disagree. And I would like to hear why you disagree.

MR. ASSAF: Respectfully, I am happy to get you additional law on this.

THE COURT: No, we are not. We have briefed this, we are living with what we are arguing today.

MR. ASSAF: But the issue is not a party's subjective understanding of what the regulatory environment is.

THE COURT: It is an objective. We agree.

MR. ASSAF: I agree it is an objective. So whether Wyndham thought X, Y or Z is irrelevant for the fair notice argument on this motion to dismiss, because it is an objective standard as to whether a

party would be put on notice, because if Bonzai Auto Sales said I had no notice, they may have an argument on summary judgment because of the compelling equities, but the Fox cases, the OSHA cases, all go to a challenge. In fact, they mentioned the CO 2 cases, whether the greenhouse gas cases, whether EPA can regulate greenhouse gas. DC Circuit just decided that.

A whole Army of parties came in and said, this is an issue of fair notice, and it is now, cert has been granted by the Supreme Court.

But the Court never said, oh, let's look at Motorola and determine whether they believe the regulations were sufficiently clear as to the prohibited conduct. It is what do the regulations, as an objective matter, tell the community as to what is prohibited? That is the standard. My client's knowledge, other client's knowledge, amicus knowledge, all are relevant as to whether fair notice is met.

That is why I keep coming back to the principle, the bedrock principle of the administrative law.

Your Honor, with all due respect, I hate to predict things, but the Third Circuit would, if they went up and said this is our regulatory scheme, we

published a pamphlet and we think you have to do what is reasonable. With all due respect, your Honor, under Dravos and under this 2008 Beverly case, I think it sits up there for a nanosecond in front of a panel.

They are saying go back and publish a regulation. You are an agency with rule making authority and come back to us with that. But as opposed to my challenge of it, anybody could challenge the regulation, and so I get to, I know district courts are struggling, you have a lot of things. What is the path here?

And I actually think the clearest path in this case is, and it protects the policy issue that you have been raising questions about, the clearest path in this case, your Honor, is to have the FTC say go back and issue regulations. You say you have a pamphlet. You said you have consent decrees. Put it all together and publish it and let people testify or give comments about it, and then, then, what do you have to worry about? You will never have another argument like this on fair notice because you would have published what is prohibited.

And so, your Honor, the clearest path is to say, you know what? I agree with Judge Fisher.

Publish a regulation. Make sure it is not vague, and then you could pursue data security, if you decide the first issue that they have standing. Even if they have standing, your Honor, you should make them publish a regulation, and say, tell people what is prohibited by the conduct, because it is an objective standard.

And then, your Honor, I like it here, I like appearing here, but I won't be bothering you. I would go right up to the Third Circuit on that issue, if there is an argument about it.

But as to me, I will be candid with the Court, it can't apply to me for 2008 conduct, and it can't apply to other companies prior to the regulation for 2009, 2010 conduct. The whole purpose of fair notice under the Supreme Court cases is that prior to bringing enforcement action you have to give them a piece of paper saying what is the prohibited activity, or alternatively, how do you stay safe and stay out of our aim?

So your Honor, on this issue, I would say, I can, if I may continue to the guidelines. I know you raised these as well.

THE COURT: Yes.

MR. ASSAF: May I approach the podium?

THE COURT: Certainly, counsel.

MR. ASSAF: I picked out the section I thought the Court and the FTC would talk about. A couple of points on passwords. Number one, no rules or regulations. There is certainly a pamphlet out there.

Number two, I think, and I could be corrected, I think the first indication that there was a pamphlet out there was in their opposition brief here in New Jersey as opposed to Arizona.

Three, it is very unclear when this was published and whether it was published at all before the conduct in question. It could be. The FTC could fill me in on it, whether it is pre 2008 or not, but whatever that is, this type of document that says here are some guidelines. It starts off actually saying, here is a guide to this.

THE COURT: Counsel, let me just say, for the record, you can put that up. Everything you said, it is unclear when this was published. We don't know, all of those smacks of issues of fact. All of that says, at least not issues of fact, we have to explore this in order for us to argue at a later stage something that sounds dispositive in nature.

MR. ASSAF: As first blush, your Honor, but

not when it is an agency of the United States taking agency action. They have the burden to show what they are doing is permitted before a company has to engage in discovery. They have the burden. In fact, when they said, oh, I am thinking about it. Page 3 of the guidelines might be implicated by paragraph 24 of the complaint.

Your Honor, that is not in the complaint at all. Okay. And so if she just shows the problems with not having ascertainable guidelines. If they want to adopt this, your Honor, they should do a couple of things. If I may be so forward. Say our guidelines, we are issuing a proposed regulation, we are adopting our guidelines. We are adopting certain private guidelines, like the SEC has done, and we are doing X, Y and Z.

Could we have your comments or could we have your testimony on that on how it impacts?

Then, your Honor, we are in a much different situation.

But I don't think, under fair notice, that it is my burden to come in at this stage and try to cobble together what the state of affairs is for the FTC's regulatory scheme. They are an agency of the federal government. They have to come forward under

the statute, again, they have rule making authority, publish a rule and tell me what is prohibited and what is allowed.

And again, your Honor, their argument is well, we can't get into too much detail. All right. But let's not have that debate in front of an Article III Judge. Let's have that debate with the actual rules and regulations. In other words, we are all shooting in the dark here because they don't want to publish a regulation. Let's publish the regulation and see what it actually looks like.

So your Honor, I would say the guidelines, the pamphlet does not get them there, and we have looked. I haven't found any case law supporting the notion that an agency pamphlet constitutes rule making under even Magnuson On Rule Making or other rule making that Congress sets forth, I come back again to rule making. Congress gave them rule-making authority. So if they want to do something, they have to publish the rules.

And this is not a summary judgment issue. This is an issue for today. And so if you decide, there are two ways on this issue.

THE COURT: Or reserve on fair notice.

MR. ASSAF: If you decide fair notice against

us, then the record is what it is. And nothing else is going to be developed because they either haven't published the regs or rules, the only thing they could do, I submit, is come forward and say here is what we think the regulatory scheme is, your Honor. But this case is so far, so much more extreme than Beverly, I think under Beverly, we win. And I wish I had cited the case. I am kicking myself for not doing it. Because there is a regulation there.

THE COURT: Well, the argument is there, counsel. I appreciate it.

MR. ASSAF: Finally I wanted to pick up a point. They mentioned the NLRB case. It is the NLRB case from the Third Circuit, that does have a special meaning under law. The NLRB general duty and good faith negotiations are looked at as contract matters as opposed to administrative law matters. So under Third Circuit precedent, that is a bucket of cases that is different than the normal administrative law cases.

It doesn't concern agency action under the APA.

And I have one more point, your Honor. Oh. Industry standard. I want to be clear, is that I think I said, and I hope I said that the irony of

today's situation is that the only agency, Homeland Security, Commerce, to published ascertainable guidelines as of today, I am feeling pretty good that we couldn't -- they couldn't use those guidelines against us, okay, because it is when they published.

So as of today, for fair notice purposes, I would look at them and say I think I have a safe harbor in those because I think I comply with them today. So that is what I was trying to say. That is again the whole purpose of fair notice is that I now know I have something I could come into court and say, as of 2013, I have these regulations. And I complied with them. So you can't take any adverse action against me.

Thank you, your Honor.

THE COURT: Any response? We are going to move along. Any response from FTC with respect to any of the issues?

MR. MORIARTY: Your Honor, I will keep it short.

So I will reiterate, it is within a agency's informed discretion to proceed by ad hoc litigation for rule making. Counsel believes the FTC should proceed by rule making. That point is clear, they believe that we should, but that it is within

the agency's discretion to choose.

And the one other point I would make is this idea, I think counsel was saying that for every unfairness case that the FTC brings, there must first be a rule. And that is a very dramatic argument. And I don't think the argument was just on data-security cases. I think it was all unfairness cases. I think in order to be consistent that has to be their argument. That is, I would say, I don't have an estimate, I think that is 90 percent of the FTC's unfairness cases including all of our competition cases which essentially require a court to evaluate the totality of the circumstances to determine whether a company was engaging in an unfair trade practice or an unfair collusion between horizontal entities. And the same is true with consumer protection. We bring cases all the time for unfairness that do not have a predicate of a rule.

Thank you, your Honor.

THE COURT: Okay. Now we move to issue three, whether unfairness is adequately pled by the FTC. And Wyndham will open with argument with respect to that.

I would state for the record, state a claim for unfair practices under Section 5 of the FTC Act,

the FTC must plead, one, that an act or practice caused or is likely to cause substantial injury to consumers; two, the injury was not reasonably avoidable by the consumers, 'and three, that the injury was not outweighed by countervailing benefits to consumers or competition.

And the issue now before the Court is whether the FTC has adequately pled.

MR. ASSAF: I am spending a lot of time up here, your Honor.

All right.

THE COURT: Understanding the Court at this point is looking at the facts in the light most favorable to the nonmoving parties, we are really going to be looking at what the complaint is, in particular I think paragraph 32 and paragraph 40 are what the Court is at least considering, and I want to hear comments, but the Court will allow counsel to raise this issue of no substantial consumer injury.

MR. ASSAF: Thank you, your Honor. Starting with the consumer -- the statute. The standard of proof is that the practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by the benefits.

So there are two issues here. One is the pleading of whether the Wyndham alleged data-security deficiencies caused the consumer harm. And I would first say, your Honor, that as you know, the complaint is very careful, it says $10.6 million fraud loss.

Now, maybe I am just being overly sensitive. But they don't say $10.6 million in consumer fraud loss, and I would argue that there is a reason for that. The reason is that federal law protects credit card users up to 50 -- in excess of $50. So I understand, though, well, you could have then $50, and that could add up.

Now, this is where I do think there are two different standards for private parties as opposed to government. I don't think the government can plead around by careful omission that which they know to be the truth. And if they are forced to amend, to amend, your Honor, they need to amend because it is, they conducted an investigation, by the record here, they have all these consent decrees, and they dealt with hard brands all the time. And they know in addition to this that every major card brand exempts the consumer from the $50.

That is why I said it is different than a private party trying to get past a motion to dismiss.

I would argue, especially as a federal agency, that they have an obligation to plead those facts even if they are inconvenient for them. And that is why I think the $10 million fraud loss, my interpretation of that is that they think that the banks, the card brands, Visa and Mastercard, may have lost that money, and they also leave aside, by the way, whether they were reimbursed by Wyndham.

But they already know all of this from the investigation, your Honor.

So I would ask that on issue one, the consumer fraud loss, that they have to plead precisely that which they know, and they are not going to be able to get around discovery. It is a different obligation. You know from your former days --

THE COURT: The word "precisely" is concerning me, counsel.

MR. ASSAF: They know they can't just ignore, when they say $10 million in fraud loss, there is a reason I submit they don't say $10 million in consumer fraud loss, because if -- unless it is consumer fraud loss, they don't meet the elements of the statute that say substantial consumer injury. If it is J. P. Morgan that has the $10 million in loss, they have no jurisdiction to bring the unfairness claim. So that

is, at the end of the day, whatever they know they know, we will leave that aside. But they have to plead consumer fraud loss, not just fraud loss in the abstract.

THE COURT: So what is your argument with respect to that? Because, are you saying that the Court must require them to amend, based on what they know now? That I have a requirement to make them amend their complaint?

MR. ASSAF: No, I would hope they would amend as to what they know now. I think they have a requirement to plead $10.6 million in consumer fraud loss as opposed to the artful phrase, $10 million fraud loss. It is the whole point of, is it the banks? The credit card companies? Or is it the consumers?

And again, your Honor, this is a matter of public record. Unlike a lot of data breach cases where consumers have brought actions against the company alleged to be involved in the breach, no actions here. Notify the consumers, notify the state attorney generals. That is why this becomes all the more informed. Where are these consumers that suffered the fraud losses? We are not hearing about them.

So that would be point one in terms of the pleadings, that they have to talk about exactly what the fraud loss is.

The second point of the pleading, your Honor, goes to causation. That is your paragraph 32, or what you reference as paragraph 32.

Paragraph 32 states as a result of defendant's unreasonable data-security practices, intruders were able to gain unauthorized access to the Hotels and Resorts corporate network, and the property management system servers of 41 Wyndham-branded hotels, twelve managed by hotel management and 29 franchisees of Hotels and Resorts. This resulted in the compromise of more than 500,000 payment card accounts and the export of hundreds of thousands of consumers payment and account numbers to a domain registered in Russia. I think there are two points on causation here.

One is that they need to plead, and I do suspect, I do argue a heightened standard, especially after an investigation that they have undertaken, that the alleged deficiencies caused the breach and caused the harm. Because, your Honor, I think what, as I read the complaint, they say there are these alleged deficiencies, and all the card brands, or all the

consumers had their information taken from the hotels.

There is, my view of the plaintiffs don't say these alleged deficiencies were a cause of the breach. And the reason I say that is I am going to get back to the criminal complaints which again, in this Court, the Russian cyber criminals, is kind of the same playbook, they took sophisticated, they put sophisticated malware on, put it in a back door, and why I think this is so important for pleading purposes is that I think the FTC needs to plead that there were alleged deficiencies and those alleged, those specific alleged deficiencies caused the briefest and the harm to consumers.

There are my two arguments. Substantial consumer harm needs to be explicitly pled; and two, that they need to plead that these alleged deficiencies caused the alleged harm.

THE COURT: Don't they plead that in the complaint already, in terms of, we look at paragraph 24, and then they cite to all these points. Isn't that pled? Aren't they saying that indeed by failing to use readily available security measures to limit access between and among the branded hotels property management system, the hotels corporate network and

the internet, such as employee's firewalls, B, C, D, E, F, through J. Maybe I am missing something. Aren't they saying that it is because of these failures that indeed, when we then turn to paragraph 32, they resulted in a compromise of more than 500,000 payment card accounts, and the export of hundreds of thousands of consumers payments. What do you say is missing?

MR. ASSAF: Your Honor, I apologize. Maybe I am missing it. I haven't seen the causal link between this precise -- and maybe it is, maybe it is, now that we have read 24, maybe it is 24, the causal link, that these caused the exact theft of the information. But I guess I have always come at this, if they are repleading on consumer harm, they may as well try to replead the exact alleged deficiencies.

THE COURT: Okay. I see your argument.

MR. ASSAF: That is what I am trying to get at. They say there are all these deficiencies. I want them to tell me what deficiency it was that caused the alleged --

THE COURT: They haven't done discovery. They are going to say to me in a minute, Judge, we need to, of course we will get to the motion to stay in a couple, at this rate in a couple of hours, but

you know, my point is, I think the other side is going to say, Judge, in order for, they are asking us to plead with such specificity, and we don't really have access right now to this critical information. We need to get this critical information and to put that on us is really unfair. I anticipate that will be an argument.

MR. ASSAF: I think they will say that, too. I think that would be reasonable, except that they had an investigation, that was within their power, they conducted it, they brought the complaint saying these were the problems.

They can't have it both ways. They can't say we know what our inadequate data security practices are and we are going to file a complaint against you alleging them and then say but we don't actually know the exact cause of the breach. Because if it turns out, your Honor, that they know that the same Russian cyber criminals used a sophisticated malware to back door, like they did in the indictment in their case, I know I am using the word fairness a lot, but if they know that, your Honor, they can't just go fishing for discovery, and so I would say tell me what exactly you have determined, since you brought a complaint, is the problem and how that caused it. Because with all due

respect, your Honor, I think they have to replead consumer injury no matter what.

THE COURT: Counsel, you say again that the requirement that they plead with more specificity, you say is because the Court should implement the higher standard?

MR. ASSAF: Yes, your Honor.

THE COURT: Okay. Before you sit down, counsel. There were some argument in your brief with respect to this issue of whether the injury was not reasonably avoidable by consumers. That is not really, are we taking an issue with respect to that, that element of the standard?

MR. ASSAF: I think that is going to get into the deception issue so I will address that during deception.

THE COURT: Okay.

MR. ASSAF: Thank you, your Honor.

THE COURT: Counsel. Mr. Moriarty.

MR. MORIARTY: Thank you, your Honor.

THE COURT: Do you need to go back and plead with more specificity, sir?

MR. MORIARTY: Your Honor, I think actually the complaint does more than we give it credit for. I agree with your anticipated criticism which is that we

haven't conducted discovery yet. And I dispute, there has been a lot of characterizations about the nature of the investigation. I just don't think those are particularly appropriate for consideration. We have not conducted discovery on how they spent the money that they claim to have spent during the investigation and it is just not something that we need to discuss, and it shouldn't affect where we are right now.

I would say that, as a factual matter, if we are going to get into the investigation, the FTC sent Wyndham an access letter which they responded to in part but there was never any formal discovery in this case. When we issued formal discovery because we needed more information, they moved to quash the discovery, and then instead of pursuing that motion to quash, they filed this case in Federal District Court. We haven't had our opportunity for formal discovery yet.

But I think that, I wasn't even on the case during the entire time of the investigation, and the parties can go back and forth a lot about who did what during the investigation. I think it is all kind of irrelevant.

So as far as causation goes, paragraph 24,

which identifies ten vulnerabilities on the Wyndham network that were caused by the unreasonable Wyndham data security practices, in paragraphs 25 through 39 which describe the three breaches, in almost every instance the paragraph aligns to a particular vulnerability.

For example, in paragraph 26, it addresses password complexity, because the password were susceptible to brute force attack. Paragraph 27, it talks about 212 user lockouts which should have alerted the IT people at Wyndham they were undergoing an attack. If they had good detection for intrusion, for potential intrusion, which is another vulnerability we identified in paragraph 24, they would have been able to respond to that.

Same with paragraph 28, refer to firewalls and segmentation. Paragraph 29 refers to the fact that there were vulnerable computers on their network that weren't getting security patches. So to go through, I could go through all of them. The main point here is there is a direct link between the vulnerabilities identified and the breaches.

The last point I would make so far as federal law and credit card companies policies regarding zero liability, it is a question of fact, not that these

policies exist, not that the law exists, but in order for the law to work, someone has to detect that fraud, whether it is the credit card company, or the consumer, and the credit card company has to acknowledge and agree that in fact that fraudulent charge was a fraudulent charge. And not all credit cards immediately accept a consumer's assertion that there was a fraudulent charge on that card.

These are questions of fact. We have alleged separately from where we identified $10.6 million in fraud charges, we separately allege in paragraph 24 unreimbursed fraud charges. We are not saying $10.6 million in unreimbursed fraud charges, but we do allege separately that there were unreimbursed fraud charges, which is to say that consumers acting reasonably under the circumstances were faced with unreimbursed fraud charges.

In addition, your Honor --

THE COURT: Where do you allege that, counsel?

MR. MORIARTY: That is paragraph 40. It is just, at the end of the same sentence where we --

THE COURT: I thought you said paragraph 24. Paragraph 40.

MR. MORIARTY: 40, line 5. As far as, we

identified 600,000, we said over 600,000 payment cards were stolen, and those include debits cards and the law, they didn't say anything about debit cards in their presentation. In the law, and card brand policies are different on debit cards and it is not true that in all circumstances debit card companies will provide for zero liability for fraud charges.

And then the last point I would make is that this case is not exclusively about the unreimbursed fraud charges. This case is about because there was $10.6 million in fraud charges, consumers faced other injuries, including loss of access to credit, loss of access to funds, when their bank accounts were temporarily frozen or depleted, reasonable mitigation costs, including paying for credit monitoring and the time, trouble and aggravation spent undoing the fraud and paying for injuries. These are what we allege in the complaint.

THE COURT: Forgive me, counsel. In its reply they said some of these lawsuits cannot be viewed as injury necessarily. You say what?

MR. MORIARTY: As I understand it, I think you are referring to the Reilly case?

THE COURT: Yes.

MR. MORIARTY: The Reilly case is a lot

different than this case. We alleged more and different kinds of injury than the plaintiffs did in Reilly.

Most significantly in Reilly there was no misuse, they did not allege misuse. By contrast, the FTC alleges misuse in this case, some of it being reimbursed, but misuse nonetheless, which gives rise to some of the unrelated injuries, including some unreimbursed fraud charges, the time and trouble spent undoing purchases and credit monitoring.

Second, the Reilly Court's holding that mitigation expenses were not reasonable was based on the fact that there was no misuse, potential misuse was merely speculative. In this case misuse isn't just nonspeculative, it actually happened. In Reilly the Third Circuit says the present sense is actuality, not hypothetical speculation. In this case the FTC's complaint passes that test because it identified actual misuse.

THE COURT: All right, counsel.

MR. MORIARTY: That is all I have unless I you have other questions.

THE COURT: No, I will probably have additional questions, depending on the response.

Counsel, again, we are looking at as pled.

When I look at paragraph 40, the language there is right after the 10.6 million in fraud loss, it says, consumers and businesses suffered financial injury including, but not limited to, unreimbursed fraudulent charges, increased costs, and the loss access to funds or credit.

Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm. I know you argue that some of those, lost time, lost access, may not necessarily constitute an injury that they can rely on, and you think it is one of monetary injury. Let me hear you a little on that and your position with respect to paragraph 40, the way it is pled.

MR. ASSAF: I am surprised because the first, this is the first time they have walked back from the $10.6 million number. It has to be in the complaint, 10.6.

I stood up and said, your Honor, I am skeptical of that. I have nothing except my lawyerly instincts to tell me that is being creatively pled. They walked back from that, and said of course the $10.6 million isn't all consumer losses. Then they point to paragraph 40 and say there is $10.6 million in fraud loss and consumer and businesses suffered

financial injury. Consumers and businesses. It is substantial consumer injury. It is not business injury. It is substantial consumer injury.

So the $10.6 million number we know that is no longer the applicable number. And then what they try to do is say, oh, it is consumers and businesses. Exactly what I said when I came up here before is that my suspicions tell me that that is the card brand and not the consumers. So if they have --

THE COURT: But even if there was some consumers, again we are at the pleading stage. Even if there were some consumers that inevitably did not get reimbursed, even, for say hundreds of dollars, all right, I mean, you would say that is not substantial injury?

MR. ASSAF: Yes. For the FTC to pursue an enforcement action for substantial consumer injury, I don't think it can be two people at $50. I don't think that that is the purpose of the Act. I don't think that is the purpose of unfairness statement. I don't think that is the exact -- remember, they are bound by the statement on unfairness that says substantial consumer injury. If they had two people out of this $10.6 million at $50, that doesn't meet the standard, your Honor.

THE COURT: Well, you cite in your brief at page 9, in your reply, you talk about the FTC Chairman Miller, and I just want to look at that section of your brief for a second, because in just taking this directly, in a 1982 letter to Senators Packwood and Katzen, FTC Chairman Miller reiterated the Commission's view on what constitutes a substantial injury. As a Federal body, the Commission believes the concerns should be with substantial injuries. Its resources should not be used for trivial or speculative harm. Substantial injury involves economics or monetary harm and does not cover subjective examples of harm, such as emotional distress or offenses to taste or social belief.

And you cite to that.

Well, it does, I mean, I looked at that, and I just, again, we are talking about monetary loss. It may just be 50 or a hundred, but what if it was, as they said, there were breaches of hundreds of thousands of card holders' information? We don't know because, again, discovery hasn't been had. But I mean, if you put them cumulatively together, is there not monetary loss and would then this cite in your brief not really help me in terms of what substantial injury is?

MR. ASSAF: No, your Honor. First of all I think the cite on emotional harm and noneconomic harm is consistent with Reilly. That part of the pleading cannot be forward. But in terms of this issue, in terms of if 600,000 numbers were accessed, and consumers didn't actually lose money, it actually, it is analogous to Reilly in some ways in that it says their credit card statement, that is my take away from Judge Aldisert's opinion in Reilly where he says your credit card statements are the same now as they were two months ago.

And so here, the fact that Russian cyber criminals took 600,000 numbers, that can't be the standard. It has to be substantial consumer injury under the statute, and the statement on unfairness. And we know that, we know that because that is what the statement says, but also, your Honor, all these other hacking incidents that I talked about, including the criminal indictment down the hall, hundreds of thousands, if not millions of credit card numbers were taken. That can't be --

THE COURT: But there was no misuse in Reilly, was there? There was no misuse in Reilly.

MR. ASSAF: I agree.

THE COURT: We have misuse here. Let's

assume arguably, I don't know what discovery is going to bare out. But what if the credit -- doesn't the credit card holder have to advise the credit card company within 60 days of the unauthorized, I am just wondering, is there a time limit that they have to advise, I have fraudulent charges on my card?

MR. ASSAF: I think that is the case, your Honor, but I also know that the -- we notify the credit card holders and we notify the card brands, and in some cases the card brands notified us saying we think there is a problem here.

Your Honor, it is not -- the notion that a couple of people who weren't reimbursed, who didn't get reimbursement can form the basis of an action for a substantial consumer injury, if there are a handful of people who for some reason, whether it be administrative or otherwise, can't get their $50 back, we started the discussion about the FTC's mission to protect consumer hard, substantial consumer injuries. We are now talking about the FTC now trying to plead around the notion of how much consumers, they know this --

THE COURT: But you are saying at a pleading stage they have to plead with such specificity, I don't think you can cite a case to me that says they

have to plead with the amount of specificity you are currently advocating. The reality is we don't know. Discovery has to play out. They have to see, was it hundreds of people that weren't reimbursed, what is the difference? Is it five people, is it a hundred? Is it if it is hundreds of people that weren't reimbursed and you cumulatively look at that number, does that amount of substantial injury. Arguably, based on what I am reading in a footnote that you provided, that goes beyond emotional distress. That goes beyond. That is monetary damage. And you can't tell me that a hundred, or, you know, what is the barometer, what is the gauge. How much is substantial injury? Can you provide that to me in terms of a monetary amount?

MR. ASSAF: Well, I could tell you it is not $100. But their pleading requirement under the statute, your Honor, and under the statement on fairness, they have to, in order to bring an enforcement action, say, determine, prior to bringing the action that there was substantial consumer injury.

So it is not, I know I am the moving party, but I am just moving saying they haven't met their statutory burden to show their substantial consumer injury. In fact, I think it is worse because I think

you just heard counsel for the FTC say the $10.6 million, that is not all consumers. That is business and consumers. So your Honor, I have a statute that says substantial consumer injury, they have to plead it.

So you are asking me what is substantial consumer injury? I am in the same position as I am on the regulation. If I had a pleading that said it is X hundreds of thousands of dollars we could then have a debate.

But it is certainly not fair for a defendant to say I don't have this information. They do. They have a statutory requirement by Congress for substantial consumer injury and they have now stood up in front of a Judge and said the $10.6 million, that is not it. It is something less than that.

THE COURT: Okay.

MR. ASSAF: Now, the final issue, the reasonably avoidable one that you raised with me, your Honor, that actually is in this section. And the reason why, that is also an element of substantial consumer injury, whether it is reasonably avoidable. Your question about, if consumers were informed, and the card brands were informed, and there are a handful of consumers who didn't then follow up, it goes

directly to reasonably avoidable injury.

THE COURT: Okay. But here is the question I had on reasonably avoidable injury. And I want to hear from both sides on this. When I read it, as I looked at it, maybe I am wrong and counsel will tell me if I am wrong, please do so.

When we look at that, the injury was not reasonably avoidable, the way that one reserves a room nowadays, you have to provide the hotel with a credit card number, even if you want to pay cash. A hotel requires that you give them, in order to reserve that room, your credit card information. All right. I think that is the way, we all can agree on that. Right?

So how am I as a consumer going to avoid the injury, that being that all my private information was hacked and taken by criminals in Russia, if I have no choice but to give you, the hotel, my credit card information, or guess what, I don't get to reserve a room in Arizona? So I am just wondering, we are talking about the injury, that being the loss, and you analyze it in saying, well, the credit card consumer calls and notifies the company of fraudulent charges, they are going to be exonerated from paying any of those charges. But when I look at injury, that being

the injury as cited in 32, and in 40, that being the information that was taken, unfortunately, as I -- I can't reasonably avoid it because in order for me to reserve a room, I need to provide this information.

So am I reading that wrong? I am looking at the wrong injury? And if so, tell me.

MR. ASSAF: Yes, your Honor. With all due respect, that approach, the question is not whether using a credit card is reasonably avoidable. That is not --

THE COURT: No, hacking, taking my private information, whether that injury, taking my information, I can't give you anything other than that information in order to reserve the room.

MR. ASSAF: Then there are three separate things. Giving your credit card to the hotel. Is that reasonably avoidable? I suspect it is not, but I think it is also not an element of this case.

I think then you get to whether the hacking itself caused a substantial consumer injury.

Or then the third issue of whether there is actual substantial consumer injury as defined by economic loss.

Issue two is not covered by the statute. There has to be, I mean, it is not only, I would

argue, this is the whole theme of actual injury. Okay. It is more than just losing, you know, that have your credit card out there and you have the time and expense. That I think is taken care of by Reilly and other cases. But it is actual substantial consumer loss.

That is the injury that the FTC has to plead in order to comply with the statute. So they have to plead that there was actual substantial consumer injury and that it was not reasonably avoidable. And so that is all, I am just asking that they comply with the statute and the statement on unfairness, but that is the key here. It is not just to say there was fraud loss and now we get to go forward.

Finally, your Honor, the debit point. Can we put up slide 102?

I just want to hopefully get rid of this issue. I know we briefed it. That the debit issue is covered like the credit card issue under federal regulation. And more importantly, your Honor, this does go to a pleading issue. There is no allegation in the complaint that pin numbers were taken. None at all. There is no -- you know, when you go into, you sometimes swipe your credit card or you do the debit, you do the pin number. There is no allegation in the

complaint, so this is a total red herring, as is the time and effort, the emotional distress issue. So when we talk about pleading issues, I don't think they meet substantial consumer injury as they conceded. That is not accurate in the complaint. They can't lump together businesses and consumers and meet their --

THE COURT: When did they concede that?

MR. ASSAF: When they got up and said we lumped together in paragraph 40 businesses and consumers. That is not what the statute, they are not there to protect substantial business injury -- substantial business injury is not part of their mission.

THE COURT: Okay. Mr. Moriarty.

MR. ASSAF: Do you have any questions? I would be happy to answer.

THE COURT: Not yet, no. Thank you, counsel Mr. Moriarty, have you conceded that the 10.6 million is not part of the loss figure in this case? Is that what you did when you stood up?

MR. MORIARTY: No, the 10.6 million dollars are the unreimbursed fraud charges. As a factual matter, it is just one card brand. But I understand we can't address that it. It is a predicate for the

loss which addresses the Reilly concern, which is that there wasn't misuse in this case. Any other injuries including monetary injuries flow from misuse.

In addition, there were unreimbursed fraud charges to the extent it is consumer and business, under the FTC Act, the FTC can protect small businesses. So the allegation refers to small businesses that often book rooms for their employees with their credit cards that also suffered the same loss of their payment card information as a result of the breaches.

On the reasonable avoidable part, the point that you made, consumers certainly would not have known that Wyndham had unreasonable data security practices in this case, especially because, as we allege, we alleged they had unreasonable data-security practices. We also allege that in their privacy policy they deceive consumers by saying we do have reasonable security data practices. That is one way consumers couldn't possibly have avoided providing a credit card to a company --

THE COURT: Can you walk me through -- I am sorry to interrupt you, counsel. That is why I apologized this morning. Can you walk me through the injury that you say the Court is looking at and

whether that injury then is reasonably avoidable?

MR. MORIARTY: Sure, your Honor. The injury we have alleged in paragraph 40 that is not reasonably avoidable, all the injuries is not reasonably avoidable, include unreimbursed fraud charges, the loss of access to funds as a result of frozen or depleted bank accounts, even if temporary, temporary loss of access to credit, and the cost of reasonable mitigation, and then we also allege injury in the form of time, trouble and aggravation dealing with unwinding this fraud, and with re-establishing recurring payments after the credit cards have to be changed for hundreds of thousands of consumers.

As far as that last point, the time trouble and aggravation, I dispute the characterization as emotional harm, or not covered by the FTC Act. In FTC versus Niovi, which is a Ninth Circuit case, there was a very similar set of circumstances, and the Court found that even if consumers were fully reimbursed or raised on their debit accounts as a result of unfair data security practices by the defendant in that case, even though they were reimbursed, the time, trouble and aggravation of being reimbursed constituted a harm under the FTC Act.

THE COURT: So your point as to whether it

was reasonably avoidable by the consumer, you would say they couldn't because they were relying on a statement and assurances by Wyndham that they were taking reasonable -- what was your -- Let me not put words in your mouth.

What is your point with respect to reasonably avoiding?

MR. MORIARTY: The point on reasonable avoidability we make in our brief is really just about the injury, not about the choice to use Wyndham. I did make that point just now. But the real point is that consumers suffered substantial injury because their payment card information was taken as a result of Wyndham's unreasonable data-security practices.

And then because it was taken there were $10.6 million in fraud charges, some of which are were unreimbursed, there was the time and trouble spent unlining the fraud, re-establishing credit, recurring payments, loss of access to funds, as well as reasonable mitigation expenses. Perhaps we should have briefed the debit card issue more.

My understanding is once you receive your notice from your bank, you are considered on notice of any fraudulent charges. So the 60 days that was referred to in the statute starts then, and so again,

this is a factual issue. This is not an issue for a motion to dismiss. But I can conceive of a situation where someone has a $4.00 charge that they don't notice and 60 days passes from when they received that charge, at that point the statute no longer provides liability cap. So after that 60 days, if there is an additional charge beyond the $4.00, a thousand dollars, $500, anything, that is not reimbursed by statute.

Thank you, your Honor. Do you have any other questions?

THE COURT: No. Thank you, counsel. Anything else?

MR. ASSAF: Your Honor, I understand we have argued this point. But I think that the last statement by the FTC illustrates why the pleading requirements have to be met. A federal enforcement agency doesn't get to stand up and say I can imagine there are situations out there. You have to plead it. You can't say, well, the law might be what it is, but I can imagine this.

They have a pleading obligation, your Honor. And they haven't published regulations, they haven't published rules. I have argued that. Now we are at a stance where they are saying I don't have to plead it

because I can imagine situations where it occurred.

With all due respect, I don't think that is the standard for a federal enforcement action. I think we have to have a standard where they have to plead what they know and it has to be true and accurate.

THE COURT: I don't think we need to get into the injury is not outweighed by countervailing benefits to consumers. If either side feels they want to weigh in on that. Counsel.

MR. MORIARTY: No, thank you, your Honor.

THE COURT: Counsel.

MR. ASSAF: No, your Honor.

THE COURT: Okay. So now it is 1:16. We have been arguing since ten o'clock this morning. I would like to take a break, take a break until 2:00 o'clock.

We will come back, and deal with count 1, the deception claim, and then we will move on to the motion filed by the other Wyndham entities, and finally the motion to stay.

Thank you, counsel. See everybody at two o'clock.

(Luncheon recess.)

A F T E R N O O N S E S S I O N

THE COURT: All right. Back on the record in the matter of FTC versus Wyndham Worldwide Corp., civil 13- 1887.

We are moving to count 1, deception claim, to establish liability under Section 5 of the FTC Act the FTC must establish there was a representation, the representation was likely to mislead customers acting reasonably under the circumstances, and the representation was material.

Actually, I want to start with the FTC, and ask that the FTC go through the complaint and tell me where in the complaint you would argue you pled the case for a deception claim.

MR. MORIARTY: Yes, your Honor. Your Honor, as I understand it, defendant's main argument that we hadn't pled deception was that the allegations in paragraph 24 apply only to franchisees, and they argue that the privacy policy applies only to the Wyndham Hotel network. Is that the issue would you like me to discuss?

THE COURT: Well, I sort of feel like in the briefs we didn't really lay out the facts to support, or disprove each of the prongs that I just went over. And so what I am asking you to do is lay out your case

in terms of looking at the case -- looking at your claims, rather, as it relates to count 1. And then of course, the whole franchisor, franchisee, but I felt I didn't really have a good handle on what facts you were relying on to support your prongs of deception.

MR. MORIARTY: Okay. So the first prong is that Wyndham made a representation, and that is in paragraph 21, it identifies the Wyndham Hotel Group privacy policy. And in that the privacy policy specifically at paragraph, line 13 of the complaint, paragraph 21, on page 9. And then also it discusses safeguarding, using industry standard practices, and then paragraph 20 says we take commercially reasonable efforts to create and maintain firewalls and other appropriate safeguards.

Then it goes on to ensure that is 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. So that is the statement that we are pointing to.

THE COURT: Okay.

MR. MORIARTY: The statement is likely to mislead because as we have alleged the practices were

not in fact commercially reasonable to create appropriate safeguards to ensure that the information is used as only authorized by us and consistent with the policy.

THE COURT: Where is that in the complaint?

MR. MORIARTY: That is paragraph 24. That just alleges the litany of vulnerabilities that appear on the network because of the lack of reasonable data security practices.

Lastly, your Honor, the materiality is, this is not in the complaint because it is a case law argument, but essentially materiality comes from the fact that it is an expressed statement, and expressed statements are presumed material under FTC law. I can give you a case for that.

THE COURT: Please do.

MR. MORIARTY: Okay.

THE COURT: While you look for that case, let me understand, you say that the representation -- strike that. One, there was a representation. You say the representation can be found in paragraph 21, specifically starting at line 13 of the complaint, right?

MR. MORIARTY: Yes.

THE COURT: Then as to the second prong, the

representation was likely to mislead customers acting reasonably under the circumstances. So you would say that 24 supports that second prong that it was likely to mislead because they weren't doing these -- they were failing to -- failed to use readily available security measures, and then again those ten vulnerabilities that you lay out in paragraph 24.

MR. MORIARTY: Yes, your Honor.

THE COURT: And then as to materiality you say that case law, and you are going to give me now a cite.

MR. MORIARTY: There are a lot of cases that support that. There is a District of New Jersey cite called In Re National Credit Management Corporation, LLC, 21 F. Supp. 2nd 424 at pinpoint 441, (District of New Jersey 1998.)

It is also in the deception statement which is the FTC's interpretation of the deception authority. That is the policy statement on deception that --

THE COURT: Where in your opposition can I find -- can I find these cases?

MR. MORIARTY: No. I would say that it is not in there because I didn't see that issue raised in their brief. That we didn't state that it was

material. The FTC statement on policy is, or FTC policy statement on deception is 103 FTC 110, pin cite 174, that is a 1984 statement.

THE COURT: All right. So the reason you didn't address it is it wasn't raised by Wyndham, so you did not address it, but you again -- give me the cite for the case.

MR. MORIARTY: For the District of New Jersey case is 21 F. Supp. 2d 424 at 441.

THE COURT: Anything else?

MR. MORIARTY: No, that covers the pleading. I will address any additional issues they raise after their argument.

THE COURT: Certainly. Let me hear from Wyndham now.

MR. MORIARTY: Thank you.

MR. ASSAF: Good afternoon, your Honor.

So deception. The FTC, after hours of argument, seems that we are coming down to this big analytical fight. Their case is apparently all about commercially reasonable efforts, and their view is that in lieu of regulation and the new rules, rules and policies, that all they have to do is show commercially reasonable, both for unfairness and now deception.

I, focusing on deception, your Honor, what we say is that we safeguard our customers' personal identical information by using industry standard practice. Although guaranteed security is not a given, on or off the internet, we make commercially reasonable efforts to make our collection of personal information consistent with applicable laws. Two points on this. It is ours. Two, it is commercially reasonable.

Here is what we have another analytical divide between the FTC and Wyndham. I keep going back to fair notice. We have the FTC, they haven't argued it but your questions at least presuppose there is some discussion about whether it is subjective or objective.

Just for the record, your Honor, I don't think they raised that in their brief. But let's assume I think from your questions you were asking whether it is subjective. We think it is objective. Here, this is -- now, the FTC is saying, well, this is objective. Fair notice, not so much. That could be subjective. I think they are buying in to your question.

THE COURT: I think they did say objective at some point.

MR. ASSAF: That would be objective. Could I take one minute, because you raised that issue, it bothered me. We were looking at it at lunch. And they didn't raise, the FTC didn't raise subjective or that it is a fact issue, fair notice, in their brief. And I didn't hear it, but I couldn't understand what their position is, and we have looked at the cases, at least over the last hour, we can't find any case, your Honor. If you do, I appreciate you already giving me Beverly, but if there is another Beverly instance I would be happy to look at it.

We looked and can't find any case in which fair notice is either a subjective issue as opposed to an objective issue, or where courts say there is a factual issue as to agency action and whether there is fair notice.

So maybe I misunderstood the FTC and misunderstood the tenor of the Court's question, but it is clearly not raised in their brief, and it is just bothering me because it seems to be a huge issue, whether this is objective or subjective and we can't find any case law saying that it is subjective and a fact issue.

So in any event, to this issue, I think you say commercially reasonable efforts, and as the FTC

said, when they are weighing agency action, their view is, well, we want to consider small businesses and we want to consider what businesses are looking at based on their dynamic and how many employees they have. I would say if anything, your Honor, that analysis helps us, because commercially reasonable effort as determined by whom?

I would say, as determined by Wyndham, not by the FTC.

And so I don't think that this is part and parcel of their deception case, and I would suggest that there is nothing in this statement that is the hallmark of deception. In fact, the FTC versus Millennium Telecom here in the District of New Jersey, the case cite from that case which I think is crucial, the cardinal factor in determining whether an act or practice is deceptive under Section 5 is the likely effect that the promoter's handiwork will have on the mind of the ordinary consumer.

So I go back to where I started this morning. Again, the case law says promoter's handiwork. There is some sort of deceptive activity. Here, your Honor, there is no real allegation that there is some sort of malevolent, deceptive activity by, or the handiwork of Wyndham at play here. What the FTC is saying is that

we disagree with what security measures you put in. And I would say, your Honor, just as a matter of logic, it can't be that the failure to implement the data security measures that they say should be implemented is somehow this nefarious promoter's handiwork under the case law.

But leave that aside, the explanation point to that is it is in the very same policy statement where we say, we do not control the use of this information or access to the access to the information by the franchisee or its associates.

And you remember, your Honor, even their complaint says it is the Wyndham-branded hotels in which the information was extracted from. And we say very plainly that it is, we don't control the franchisee information.

So I don't think they can have it both ways, saying, well, the policy is deceptive because a consumer reads it and is deceived by the policy. But then the very next page of the policy tells the consumer we don't control your information and the FTC says, well, ignore that section. The consumer isn't reading that portion of the section.

So I would say that the policy itself is not deceptive on its face, and I think the best source

here is the international franchise association cases that talk about the relationship between franchisor and franchisee, including the Radisson case, from New Jersey, which is slide 63. I call it the Radisson case. The District of New Jersey, I think it is Judge Thompson. Judge Thompson. There is no genuine dispute that Radisson lacked both ownership interest and control over the day-to-day operations of the hotel. The right to conduct and carry out periodic inspections to ensure consistency and quality of the Radisson brand does not give rise to the power to control the daily maintenance of the premises. Courts that have addressed the issue of duty require franchisors to exercise more than a right to control uniformity of appearance, products and administration in order to find a duty of care.

The International Franchising brief says it much better than I could. I think it is pretty clear from cases across the country that franchisors should be held liable for franchisee problems

And again, stepping back why we are here.

THE COURT: You anticipated my next question which is why --

MR. ASSAF: This is such a huge issue, because this is what I call the bridge too far. This

is why we are here. That the FTC, you look at all those --

THE COURT: My question is why now? The question that I was going to ask, the one I have been asking you all, throughout the course, I am not trying to give counsel a hard time, I just really honestly think a lot of the questions in terms of how the franchisor and the franchisee deal with one another, all of these sound like issues that are better left for a later point in time, not at a motion to dismiss.

And I know that you fundamentally disagree with me, and that is fair. That is why we are having oral argument for us to flush out your position. But I mean a lot of these arguments, you know, you even say in your moving papers, counsel, page 27, and I have questions which is that you say that the security standard, defendants say the security standard is adequate or reasonable is a question of law, page 27, not of fact. And all allegations as to the same are the properly disregarded on a motion to dismiss. Where do you support the statement?

MR. ASSAF: This is a huge issue, your Honor, it goes back to the fair notice and the pleadings standards we have been talking about, and this is Twombly. This is, it is for a private party Twombly

and for the government Twombly. The FTC can't just make secure generalized allegations because that runs afoul of Twombly.

So I know you and I have had a lively exchange, it has been great, it has been a fun argument, it is why you are a lawyer, this is a good day, even though some of the questions haven't been that good.

But again, this is really, really important because Twombly, Twombly infects the government's complaint for all the issues I talked about earlier, that they can't just say, hey, we are making these conclusory allegations that these are unreasonable security efforts. It is the double whammy for me. Okay, they don't publish it, I know, talk about fair notice.

Then they say I don't even have to meet Twombly for the pleading. All I have to say is it is unreasonable, or commercially unreasonable. That is what it is. So this is more of a Twombly, Iqbal issue. I think if this were a private party I would suspect that the Court would have really hard questions about well, there has to be more --

THE COURT: Why is it Twombly? Step me through it, just as I asked counsel, Mr. Moriarty, the

question, step me through, we are analyzing it from an MTD point of view. Tell me why it is not adequate. Tell me why it is not pled with particularity. What are they missing?

If we look at what they are saying, counsel says, Judge, we say the representation can be found on page 21. Strike that. Paragraph 21, page 9 of my complaint, starts at line 13. We say that obviously it was, it was a representation that was likely to mislead customers acting reasonably under the circumstances, because they weren't doing that. What they did, Judge, is they, and they say on paragraph 24, that I have ten separate vulnerabilities, that, you know, obviously are misrepresentation, and that it was material, they argue, there is case law to support that it was material misrepresentation.

Tell me why now this is a Twombly issue, and not an issue that I think we disagree on, an issue better left for summary judgment at a dispositive stage when discovery has been exchanged and we can now look to what they are alleging the actual deficiencies are in terms of the record. But I have at least ten here saying there were deficiencies. Why is that there is not enough when you look at it from an Iqbal Twombly perspective?

MR. ASSAF: 21, they say these are the policies. These are the policies. 24, they say, 24, we decided to, or we failed to provide reasonable security measures. And they identify a number of allegations that were not reasonable.

Now, in term of Twombly, I didn't think they were simply able to say these are things that they didn't do.

It gets back to my whole causation point, that they have to address with specificity that these deceptive statements were in the mind of the consumers, for example, on 24, that a reasonable consumer would think that the available security measure, that firewalls were being used. Okay. I don't think they simply say, here is a litany of problems and it is deceptive.

The deceptive element that they have to say a reasonable consumer, having reviewed this policy, would find deceptive. And I don't think that is in here.

So under Twombly, they can't just say these are a bunch of problems. These are deceptive, and we have now cited our deception count. I think they have to do more in terms of analyzing, like a securities fraud case, these statements were made to the

investment public, that a reasonable investor relied on these on October 2, and that by relying on these, caused harm. And I don't think they do it under Twombly.

So that is why in terms of the cases, too, I come back to the notion that we would have to go through discovery to have all of these questions answered when the law is so clear that the franchisor-franchisee relationship is what it is, and so if they are going to now exceed what I think the clear law is on franchisor-franchisee relationship, that is even a higher burden under Twombly because now they have to come forward saying in the normal franchisee-franchisee relationship, we understand this is the law controlled as an equal liability in terms of appearance, et cetera.

Now under Twombly they have to do more. They can't just say I am entitled to discovery because I am making these allegations. We know this law is out there and the franchisor-franchisee relationship. Otherwise, they will always simply plead these are unreasonable standards and the franchisor is liable and thus we get discovery.

I put it the other way around, your Honor. How would I ever get, under the discussions we have

had, how would I ever win on a motion for judgment on the pleadings or a motion to dismiss? Because as I said --

THE COURT: But even that case that you are citing, wasn't that summary judgment?

MR. ASSAF: That was summary judgment, your Honor. But if you look at all the cases in the IFA brief, these are cases on summary judgment and motions to dismiss, and I would say again here, they have to come forward with some fact, some plus factor to show that outside this. Otherwise, your Honor, in two months, if I am here, and they say, you know what? All the indicia of franchisor-franchisee relationship after millions of dollars in discovery, you are right. That is where it was.

That doesn't really benefit me. The whole purpose of Twombly is to avoid excessive and costly discovery by putting the pleading party's feet to the fire before discovery begins.

THE COURT: You seem to be holding the agency to a higher standard. A heightened pleading. And I would like you to speak to that a little bit, because you said earlier, it was in a different context but I do, you know, speaking of wanting to get back to things, we were discussing issue three and whether

unfairness was adequately pled by the FTC. You started, you know, and I asked you whether this was almost a heightened standard that I was holding you to, and you somewhat said there is a difference between the private party versus a federal agency.

Where can I find that in the law?

MR. ASSAF: Yes, there are two issues. I think on this issue we are talking about, deception, that clearly sounds in fraud and I would suggest that since it sounds in fraud as cited on page 24 in our brief, it should meet 9 (b) requirements. It is deception or fraud, that is the whole purpose of Rule 9 (b). When you see the deception elements, FCC versus Millennium Telecard, July 12, 2011, we have a couple cases that support that position. Again we cited in our brief. FTC versus Lights of America, FTC v. Ivy Capital talking about when there is a deception claims there is a heightened standard. Your Honor, to be sure there is a case that disagrees with this. Out of the Southern District of New York.

THE COURT: They cite to it, right?

MR. ASSAF: Right. They cite to it. But here, one of my entire themes today has been I think we are different because we are not schemers and we are not deceivers. They need that under their

statute, especially deception.

So this isn't like phishing or check kiting or ripping offer elderly people. So once you are now in this new area, then I think it is especially incumbent upon the FTC if you are going to bring a deception claim to meet Twombly and to meet 9 (b). So that is my argument there. It does us no good under Twombly. In fact, Twombly says the opposite: At the end of the case for summary judgment the defendant will have spent millions of dollars only to be vindicated on the position that they thought was at the summary judgment stage.

THE COURT: Thank you, counsel.

MR. ASSAF: Thank you.

THE COURT: Any response?

MR. MORIARTY: Yes, your Honor.

THE COURT: You cite in your brief on page 26, you cite to a case the that held a claim of deceptive practices, pursuant to Section 5, "is not a claim of fraud as that term is commonly understood or contemplated by rule 9 (b)."

MR. MORIARTY: That's right. Under the FTC Act, in order to prove deception the case law states the FTC does not have to prove intent. That is where we are getting away from the FTC Act when counsel

suggests we have to somehow prove Wyndham is a bad guy or a bad actor, or anything like that which we are not alleging.

And in addition, it is also what makes a difference in a securities fraud case where a company has to lie, someone has to rely on that intentional lie, and be injured by it. In this case we have, the standard is simply that they made a statement that deceived consumers, whether or not they intended to, and as a result the relief that we can get is less. We don't get remedies at law. We don't get punitive damages.

Regardless, your Honor, if it did sound in fraud, we would have to proceed with particularity, which we have done here. It simply requires to us say precisely what the elements of our claim are, which we have done in paragraphs 21, 24 and the fact that we allege a difference between express statement and therefore materially consumers.

So the last point I want to talk about with deception is this idea that franchise law is somehow relevant. We argue that that is a red herring, it is not relevant at all. We allege that Wyndham made statements about how they treat their network and we allege in paragraph 24 vulnerabilities by Wyndham on

the Wyndham network. The idea that these are franchisees, that they have disclaimed what happens at Wyndham hotels has nothing to do with the core of our allegations which is that Wyndham engaged in unreasonable data-security practices on the Wyndham network.

THE COURT: Counsel, can you speak to the issues raised with the subjective and objective standard, as it relates to fair notice and that they don't see any cases that say, you know, that speak to whether it is a subjective or objective standard, and I am interested -- I know we are going backwards, back to fair notice, where I believe we focused a lot of our argument here today. Can you speak to your position, and if it is not in your briefs, and if so, why not?

MR. MORIARTY: It is in our briefs and it does relate to the deception issue because it is this idea that if they say we are going to take commercially reasonable practices, is it okay for them to say we are going to take what we believe are our commercially reasonable practices, they might not be your commercially reasonable practices. The idea that reasonable under the law is something that everyone can have a different idea of. It doesn't mean

anything. Subjective standard is simply wrong. Reasonableness is an objective standard.

When the FTC states for the purpose of unfairness that reasonableness is what unfairness means as it applies to data security, that is an objective standard. So in a way, in a very real way, the proof is the same on both sides. Unfairness requires them to take reasonable steps to protect consumer data, and as it happens in their statement, in their privacy policy, they say they will take commercially reasonable steps to protect consumer data. It is the same evidence in the case.

THE COURT: And you say again reasonableness is an objective standard.

MR. MORIARTY: That's correct, your Honor. And I think, that appears in the Vogel case, they talk about reasonableness as an objective standard. I can pull it up.

THE COURT: Can you take a moment and pull it up if you will?

MR. MORIARTY: Yes. I am not into the tech. I can just read it. I am not going to use the Elmo.

So talking about an unconstitutionally based challenge, this is at pin cite 1078. In order to uphold the regulations in the face of such a

constitutional attack, the first test of the regulation has been held to imply an objective standard, the reasonably prudent person test.

Then it goes on to say whether a reasonable person familiar with the conditions in the industry would have instituted more elaborate precautions.

THE COURT: Okay. You answered my question. Counsel. Thank you.

MR. MORIARTY: Any other questions?

THE COURT: Not yet. I might.

MR. ASSAF: It is such an important issue, your Honor, I don't think that actually responds, at least to the question that you and I were discussing, is whether it is an objective standard as to what Wyndham needs to meet to comply with their version of an enforcement action. I think the question you and I were discussing, which is critical to this, is whether for fair notice challenge, there is a question of whether there is an objective standard that accompanied the challenge of the fair notice standard or a subjective.

And we have been saying, and I think the case law bears it out, I want to correct something, I didn't mean to suggest that we can't find it one way or the other. I think if we read the cases, every

case we read is an objective standard, that you look at fair notice objectively as to what the agency does.

THE COURT: I may have posed the question incorrectly. I apologize.

MR. ASSAF: I think the FTC, they don't argue that it is a subjective standard. They don't argue it is an issue of fact. That is what I thought you were asking them. I don't think they kind of confirmed that, it is a crucial issue obviously in terms of the motion to dismiss, whether it can be decided as a threshold matter, based on record evidence of Code of Federal Regulation and publicly available materials, or whether there is a subjective standard, and I don't know, I think it is important that the FTC at least, because there is a lot in the record right now as to how it goes, but I think we are all now on the same page, this it is an objective standard, unless the FTC disagrees.

THE COURT: No, I believe. Let me let counsel for the FTC clarify. I believe that you had argued earlier that it was an objective standard. But counsel, clarify for the record, now we are dealing specifically with the fair notice issue that we addressed in our earlier argument, that you do submit it is an objective standard?

MR. MORIARTY: You know, I might not be fully on the same page, but our argument is that reasonableness is an objective standard, and we have provided fair notice to entities engaged in data security practices by stating they need to have reasonable data-security practices.

THE COURT: Okay. And then the issue as to whether there was an issue of fact was something that I actually raised with counsel, and said, well, why are we raising this now? Shouldn't we at least exchange discovery to see what Wyndham may have known, and counsel corrected me that it is not important what Wyndham knows because it is not subjective, but it is whether they had fair notice, and the only issue that I would say back, having thought about it during lunch as well, is that, well, there may be documents that indicate that Wyndham was on notice of certain things, either via consent decrees, or best practices. And if there are memos, internal memos or concerns within Wyndham, that is an issue that has to obviously play out in discovery, but it would be relevant, I believe, to the issue of notice, and whether they had notice as to particular standards that they needed to have in place.

That is I think what we were all, we were

sort of talking around each other.

But I believe counsel said that they never heard you claim it was a subjective issue. You didn't. And that they never at least saw in your papers that you were saying these were issues of fact. And I quite frankly raised that during the course of oral argument today in fairness as to whether this was something that obviously the parties needed to delve into in discovery.

So the record I think is now clear as to how this sort of all involved.

But counsel, you are looking at me kind of puzzled. I want to make sure --

MR. MORIARTY: No, that is just my face.

THE COURT: Is there anything you can shed light on in terms of any of these issues that relates to fair notice and/or your deceptive claim?

MR. MORIARTY: No, your Honor. I do agree we have alleged they have engaged in unreasonable data security practices and discovery will tell us whether they have. They spent a lot of time talking about very sophisticated malware, there is nothing they could have done to stop it. These are questions of fact.

Some of the things we might find out, we have

alleged they didn't take steps to prevent intrusions or that when they knew of intrusions they didn't take steps to remedy where those intrusions were coming from.

And these are questions of fact that we will find out through further discovery, who knew what, how did they find the information, what did they do in response to the information, how long did it take, these are factual questions.

THE COURT: Okay.

MR. MORIARTY: Thank you.

THE COURT: Counsel, go ahead. I have a feeling you may want to respond.

MR. ASSAF: I don't want to date myself, your Honor, but Cool Hand Luke and Paul Newman, stay down, stay down. I sometimes feel like that, today. In terms of staying down. I will try one more time.

This analytically, we are not, the discussion you and I are having is different than what the discussion you and the FTC is having. I am not discussing what needs to be alleged in their complaint for unreasonable data security and what has to be proven. That is not what this discussion is about.

My discussion is a constitutional one, of due process and fair notice, that a party who makes an

allegation that the agency is acting inconsistent with due process and fair notice, that is not a factual issue that requires discovery. And in fact, I haven't seen any cases showing that it is. The subjective intent of the party challenging the agency action as inconsistent with due process is one of an objective standard.

That is the discussion that is critical for what I thought was issue two today, and what I have been trying to get at, is no discovery is relevant or necessary for that.

If General Electric had a file full of memos stating that the EPA's position would be what it is, and had a bunch of actual discussions about consent decrees under the EPA's power and what they meant, it wouldn't matter a hill of beans to GE's challenge under due process. The only thing that matters is the objective standard. So that is why the party challenging it, what my subjective intent was and whether I thought consent decrees were out there and what they meant, irrelevant to a due process constitutional challenge.

That is the thing I am trying to get at is, I think, again, my view is that it would be erroneous to, that is why I asked, I am trying to get to the

SEC's position, it is not in their brief. I think it would be erroneous to assert that a party making a constitutional challenge is their subjective intent as to the challenge. That is the point I am trying to get at.

I am sorry, your Honor, for belaboring it, but it is such an important point.

Finally, on Vogel, I thought we put a pin in it before, Vogel is a case they cite for reasonableness. This is on the other side, this is if discovery goes forward or the agency action. It is a NLRB case under contract principle. The Third Circuit as well as every other Court of Appeals is very clear, the NLRB jurisprudence is factual based, and there were things in the record besides the administrative action.

You have a whole body of case law from NLRB and what good cause means and what workers' rights means, it is contract-based based on the collective bargaining agreement, and other issues under the NLRB. That Third Circuit case doesn't help them out.

Thank you for your indulgence, your Honor.

THE COURT: Thank you. Anything further from the FTC?

MR. MORIARTY: I would point out, when you or

your clerk pulls it up, Vogel is an Occupational Safety and Health case, it is under the general duty clause.

THE COURT: Let's move to the second round of the motions here. I believe we have addressed everything. This pertains to WHR. We now look at the other Wyndham entities' motion to dismiss. I will hear counsel now for Wyndham.

MR. ALLEN: Thank you, your Honor. For the record, Winn Allen on behalf of defendants.

I know you are probably glad to see a change of scenery up here.

Your Honor, thank you again for oral argument on this hearing. It is undisputed that the only defendant in this case who whose computer systems were breached, whose computer systems were alleged to have inadequate data security protection is Wyndham Hotels and Resorts, LLC, which is one of the many subsidiary companies of the Wyndham corporate family.

Nonetheless, as you know, the FTC, Wyndham Hotels and Resorts direct parent company, Wyndham Hotel Group, and the ultimate parent company, the entire Wyndham corporate family, Wyndham Worldwide Corporation.

As your Honor well knows, in the normal case,

we don't accept such imputed liability, in a typical thirties there is a strong presumption against it.

What the FTC says here is that there is a long line of cases invoking what they call common law liability under Section 5 of the FTC Act. I submit to your Honor there is a fundamental legal problem with the FTC common enterprise allegations in this case, that make it appropriate for resolution at the motion to dismiss stage, I can anticipate one of the questions your Honor might have is why now, why not at summary judgment?

The main problem is if you look at all the common enterprise cases we cite and the FTC cites, there is a common thread that runs through them. I will quote here just a few cites. Common enterprise liability applies when, quote, a judgment absolving one of them, that is the defendants, a judgment object absolving one of the defendants of liability would provide the other defendants with a clear mechanism for awarding the terms of avoiding the terms of the order. That is NHS Systems, cited in the brief, point 13, WL 1285424, National Urological Group also cited in the brief, Delaware Watch case, also cited in the briefs.

Your Honor, the FTC has not and cannot as a

matter of law allege that here. There are no allegations in the complaint that Hotels and Resorts has ever in the past resorted to the corporate forum to try to avoid a final court order, or that it is particularly plausible to think Hotels and Resorts would do that in the future.

As a legal matter, your Honor, again, we are operating at a little bit of an unknown area here given this is the first data securities case, we are unclear as to what the legal obligations of Section 5 are, if it does indeed apply to the data security. What the FTC has said is the data-security obligations they believe are in Section 5 attach to entities that collect data.

One place we cited that was a document called protecting consumer privacy in the area of rapid change. We cited that in the brief. There is another document that is cited in the brief, we didn't directly cite it for this proposition that I would call the Court's attention to, and that is the document called Privacy on Line, Fair Information Practices in the Electronic Marketplace, May, 2000 document, that is cited in Hotels and Resorts' motion to dismiss. It is not cited in our motion to dismiss.

If you look at pages 33 and 34 of that

document, the FTC makes the same point, the legal obligations imposed by Section 5 attach to entities that collect data.

Here it is undisputed that as it pertains to this case, the only entities that were collecting consumer data were Hotels and Resorts, the main defendant, Mr. Assaf was just up here on behalf of, and the independently owned Wyndham hotels that aren't parties here. Those legal obligations that the FTC believes Section 5 to impose are going to stay attached to Hotels and Resorts for as long as it is collecting consumer date. You don't need Wyndham Worldwide Corporation.

THE COURT: But I am confused. Maybe you can address this.

One of the things that the FTC says is that at some point, Wyndham Hotel Group was managing the security, the info security program for hotels and Resorts, that was anywhere between June, 2008 to June, 2009. There is an agency, again, as you know, looking at the facts in the light most favorable to the nonmoving party, there is that allegation that that was being managed by WHG. At some point I think there was a concession that WWC, and the FTC argued on page 10 of the complaint, basically pleads that Wyndham

Worldwide controlled the acts and practices of its subsidiaries including Hotels and Resorts, WWC was responsible for the data security of Hotels and Resorts network during the third breach. So there are allegations, and we are at, again, a motion to dismiss phase in this case and not summary judgment. So with those allegations, why would it be proper to let WWC and WHG out?

MR. ALLEN: Absolutely. Paragraph 14 of the complaint they do allege and I accept as true for my argument when Wyndham Hotel Group had responsible for data security at Hotels and Resorts for a period of time and Wyndham Worldwide did, as a matter of law, I submit, that that is not enough to bring them in the case on a common enterprise theory. It goes back to my distinction between entities that collect data and entities that provide data security services.

Here it is undisputed in the complaint that Hotels and Resorts, and the independently owned Wyndham Hotels, were the entities that were collecting the consumer data that is at issue here, and therefore they are the entities that are subject to the ultimate legal responsibilities that the FTC believes Section 5 to impose.

So frankly, whether Wyndham Worldwide

Corporation, whether Wyndham Hotel Group, whether a third party entity that we contracted with was providing data-security services to Hotels and Resorts is irrelevant for purposes of Section 5 liability. The Section 5 theory that the FTC has in this case attaches to the entity that collects the data, and here that is Hotels and Resorts.

I make one other point, your Honor, is that the FTC couldn't make out a stand-alone case against Wyndham Worldwide Corporation, the ultimate parent company or Wyndham Hotel Group, the company that sits between Wyndham Worldwide and Hotels and Resorts, that is because the Section 5 of the FTC Act, your Honor, is a consumer protection statute. It is directed at consumers. It prevents deceptive and unfair acts directed at consumers.

And here, your Honor, as pled in the complaint, the entities interfacing with consumers that are alleged to have made statements to the consumers and acted unfairly to consumers were the independently owned hotels that aren't parties here and Wyndham Hotels Resorts. Your Honor, I have two other quick points.

THE COURT: Before you move to your other quick points, the Court has a case, Judge Linares, it

was issued on July 12 of 2011, and that is FTC Millennium Telecards, and I am quoting from it.

"When determining whether a common enterprise exists, courts look to a variety of factors, including common controls, the sharing of office space and officers, whether business is transacted through a place of interrelated companies, unified advertising, and evidence which reveals that no real distinction existed between the corporate defendants."

And so I am guided by this case in terms of when we talk about common enterprise, why it would be appropriate at this stage, since there have been allegations, and the FTC has basically gone through in their complaint, where there is a sharing of office space and so forth. Again I ask you, understanding what Judge Linares held in 2011 and understanding that common enterprise, and those are some factors that the Court should look at, why again you think it is appropriate to dismiss now?

MR. ALLEN: Three points, your Honor.

First, the factors that you point to are only one element of the common enterprise analysis. The other one is the one I just spent time talking about to prove common enterprise liability you have to prove that there is some reason to think that the entity

will be more subject to liability.

The second is if you look the at facts alleged, one, Wyndham conducted business through a maze of interrelated companies; two, common control; three, shared office space; and four, pooled resources and staff.

I submit to your Honor that those aren't evidence of a common enterprise or ignoring the corporate forum. They are routine facts of life for modern corporate America. Pretty much any company in the Fortune 500, they will keep themselves distinct for liability purposes to have different entities within their corporate family, but they will also synergize by sharing functions and common employees. That is why a number of cases we cited in a brief, Spagnola, from the SDNY, Universal Health Services from West Virginia, routinely say that those facts that the FTC alleged aren't enough to disregard corporate separateness, particularly when you have a reason to think that at the end of the day the defendant is going to be able to use the corporate forum sham to avoid liability.

I mentioned Universal Health Services. I encourage you to read that case. It is a case under the False Claims Act. But the facts are very similar

and the Court there was applying federal common law, the same kind of federal common law this court would apply in trying to decide whether to set aside corporate distinctions. There the government sued a subsidiary and tried to amend its complaint to add a parent company. The government made the same arguments the FTC is making here: Common control, shared office space, shared employees, parent provided services to their subs. The Court rejected the government's attempts to bring liability against the subs for the two reasons I have explained to you. One is the Court didn't see there is any reasonable likelihood that the sub would try to avoid liability at the end of the day; and two, the facts the government relied on were simply routine facts of doing business.

One last point before I sit down, your Honor, is that if you look at the common enterprise cases and there are a number of them cited in both briefs. I submit to you they are materially different from this case. I am generalizing here, of course, but most of them involved closely held corporations; they were run by a single individual or group of individuals. The actual individuals who ran the companies were often included as defendants in the very case. They often

used corporate forums to shift assets and revenues back and forth and critically, in most of the cases cited by us and the FTC, there was evidence of a deliberate intent to use the corporate forum to do one of two things: One, to avoid consumer complaints, you know, some individual set up a company, it got a lot of consumer complaints, let's just set up another company and do the same thing; or two, to explicitly avoid state and federal regulatory investigations.

In a lot of cases you would have the FTC or state Attorney General file a complaint, they set up another company and move the assets.

With that, unless you have questions, I will sit down and save the rest for my rebuttal.

MR. MORIARTY: Your Honor, regarding common enterprise, I am not sure if that case involving, I guess it was a False Claims Act, I don't think it was a common enterprise case. I don't know, though. I could be wrong. I think common enterprise shows up, I think it is a unique creatures of the FTC Act jurisprudence.

As far as the common enterprise is concerned, and whether this company is likely to shift responsibility, whether we would be able to get the same relief by just going after WHR because they have

a collection responsibility, I think those are sort of besides the point. What we have alleged here are the factors that are necessary to establish common enterprise.

And then as far as the question of whether they are likely to transfer authority, we have alleged that in fact, responsibility for data security, which we allege was unreasonable in the complaint, paragraph 24, was transferred during the time of the complaint, from, I believe Wyndham Hotel Group had it initially during the first --

THE COURT: That was my question for you. In your brief you say June of 2008 to June, 2009, Wyndham Hotel Group was in charge of managing it. But we know, at least according to the complaint, that the allegations are that our first breach happened in April, 2008, right?

MR. MORIARTY: Yes.

THE COURT: I think the second breach, let me refresh my recollection, I am sure you can tell me right off the bat, the second breach then occurred on March, 2009.

MR. MORIARTY: Correct.

THE COURT: So this all predates when Wyndham Hotel Group, WHG, was managing the security programs.

MR. MORIARTY: I am sorry. I think those were during Wyndham Group managing and then in June, 2009, Wyndham Worldwide took over. Throughout the entire Wyndham Hotel network -- Hotels and Resorts owns the Wyndham hotel network. They always own it. That is our allegation. That is what we understand.

Wyndham Hotel Group is in charge from the beginning of the relevant time in the complaint, they are in charge of data security. They are in charge from the beginning until June, 2009, during which the first two breaches happen. Then it is transferred to Wyndham Worldwide Corporation, June, 2009. I think the last breach starts to happen some time in the fall of 2009, and is discovered in 2010.

So We have alleged that responsibility for these various things does transfer. So to the extent that we are not going to look at the common enterprise prongs, we are only going to look at the likelihood of the FTC being able to get its injunctive relief against just WHR, there are factors in the complaint that suggest that this type of authority, or perhaps even the ownership of the Wyndham Hotel network can change.

More importantly, we alleged direct liability against each of the Wyndham entities. So even setting

aside common enterprise, all the named defendants belong in this case.

For Wyndham Hotel Group, the policy at issue in this case says it is he policy of Wyndham Hotel Group. The complaint also alleges, as I just mentioned, paragraph 14 that Wyndham Hotel Group was responsible for the data-security program. Wyndham Worldwide is the parent corporation of, controls the acts and practices of the subsidiaries, including the named defendants in the case. Paragraph 14, the complaint alleges that Wyndham Worldwide is responsible for the data-security policies of its subsidiaries which are what are at issue in this case.

Lastly, paragraph 14, we talk about transfer of the authority, transfer responsibility for data-security program in the Wyndham Hotel network to Wyndham Worldwide, 2009.

Lastly, Wyndham Hotel management was responsible for all operations that manage Wyndham Hotels, including data security, including responsibility for data security at several management hotels that ere breached.

The complaint alleges that Hotel Management operated the websites of Wyndham Hotels, some of which referred consumers to the main website where the

privacy policy was hosted.

So what we have in our complaint is allegations of direct liability for unfair and deceptive practices against each of the four Wyndham entities in addition to a common enterprise liability theory.

That is everything I had on that. Do you have any questions?

THE COURT: No. Anything further, counsel.

MR. ALLEN: Briefly, your Honor.

With respect to the Universal Healthcare decision, again, that Court was applying federal common law, and courts applying common income liability under Section 5.

On the direct liability issue I think it is important to take them claim by claim. If you look at deception claim, which is count 1, the FTC spent a lot of time talking about with the deception claim centered around the policy. The privacy policy doesn't mention Wyndham Worldwide Corporation at all, except to distinguish Wyndham Worldwide Corporation from the entities that are actually making representations in the privacy policy.

So I don't understand how Wyndham Worldwide Corporation could be alleged to have made any

deceptive representations in this case at all.

Wyndham Hotel Management is not mentioned at all. I really don't understand it with respect to that.

On the unfairness claim again, briefly, all of the key unfairness allegations, I would say one more time, pertain to conduct at Wyndham-branded hotels, or at Hotels and Resorts where breaches were, where the computer networks were, and again, the ultimate legal liability in Section 5 is imposed on entities that collect data, not on entities that provide management services.

THE COURT: Thank you, Mr. Allen. All right. We are at the last motion. This is a motion to stay. It is filed by Wyndham.

MR. QUINN: Good afternoon, your Honor. Justin Quinn on behalf of the defendants.

I want to thank your Honor for having argument on the motion to stay.

THE COURT: Because you know, Mr. Quinn, that generally this would be something that I would ask my Magistrate Judge to handle, and I quite frankly am going to entertain it right now, but there is the common practice of this Court, both as a Magistrate Judge for four and a half years, as well as a District

Judge now, I rarely grant such a stay, and my position has always been, in very rare instances will I grant a stay, and I would like to hear from you now why you believe the Court should grant the stay in light of the journey that this case has taken, and quite frankly, we have, you know, the original complaint was filed on June 26 of 2012. There was an August 2nd motion to change venue. There was an amended complaint that was ultimately filed on August 9. And a pending motion to dismiss that was filed on August 27.

And of course, I have done my best to bring you all to court as soon as I could feasibly do that, based on the Court's calendar. But a lot of time has gone by.

I am just afraid to let more time go by without moving the parties towards discovery here in the actual exchange. So why should I stay the discovery at this point pending my ruling in these matters?

MR. QUINN: Well, I think there are three fundamental and practical reasons that would justify a stay.

Your Honor has the discretion to stay the discovery in this case pending the motion to dismiss,

and the party making the application must demonstrate good cause.

So in this case, good cause exists for three reasons, the first of which the duration of the stay is that we are requesting here is minimal. In this case the parties briefed the issues, as your Honor noted, the Court scheduled it, today we are here for oral argument. So Wyndham anticipated that a decision on the motions to dismiss will be rendered forthwith.

And I just want to state that the FTC can't say that they are going to be prejudiced. Let me just be clear. Wyndham has expended over $5 million, and turned over well over a million pages of documents. By contrast, Wyndham has received 1,000 pages of what is effectively publicly available documents that are on the website.

Second, and fundamentally, your Honor, this case presents several, or I should say a few threshold issues which, if rendered in Wyndham's favor may foreclose portions of this litigation, if not the litigation in its entirety which would in turn absolve the need for discovery, which under settled law in this Circuit is the purpose of a motion to stay.

In other words, motions to stay pending motions to dismiss are granted when the motions to

dismiss would either narrow discovery or absolve the need for discovery. That is exactly the case here.

Finally, your Honor, I will be brief.

THE COURT: You don't have to be.

MR. QUINN: I understand.

Finally, your Honor, conducting the discovery at this juncture would be an inefficient use of the parties' resources. I am sure you are aware discovery disputes would be spawned which would in turn burden the Court. So it is for those three reasons, Judge, that good cause exists and discovery should be held in abeyance until the Court has determined its motion to dismiss.

Thank you, Judge.

THE COURT: Thank you. I take it from reading the opposition that the FTC is saying we hadn't had discovery, that we in fact have not, the defendant has not been cooperative with our request, yet we have been turning over discovery to them, and you cite to several interrogatories, I think a total of 47 requests for admissions, and 33 doc requests, that in total have been asked of you and that you have been complying with, and that all you asked for is reciprocity. Right?

And I do have a couple of questions for Mr.

Quinn with respect to some of the points raised in the brief. But let me hear you now.

MR. ZIMMERMAN: I would agree with your Honor, for the record. Jonathan Zimmerman on behalf of the FTC.

I will address Mr. Quinn's response quickly. Before I do, this case came to your Honor in a somewhat unusual posture. As soon as we filed the case in Arizona, we were ordered to begin discovery, and the plaintiffs and defendants and plaintiffs aggressively pursued discovery for nearly nine months before the case was transferred here.

During that period, we responded at length to numerous discovery requests which your Honor has outlined. In return, we received minimal responses from Wyndham. In fact --

THE COURT: What of this point that Mr. Quinn makes, that you received thousands of pages --

MR. ZIMMERMAN: They continually point to the $5 million and thousands of pages. That came up in their motion to quash the administrative subpoena which was attached to our opposition brief, the decision.

The Commission, and what I would say to that is, number 1, we don't believe that those are in any

way full and adequate responses to our discovery requests. And even if they were, Wyndham has not made the simple effort of identifying how those documents respond to our discovery requests. They simply say we produced a bunch of stuff. That should be enough.

THE COURT: So it is a document dump. You say it is not particularly responsive.

MR. ZIMMERMAN: Essentially, as the Commission found on the motion to quash, much of it was irrelevant, a lot of it did not address things that came up in the administrative subpoena. And in no way now that we are in federal court do we believe it is fully responsive to the pending discovery requests.

THE COURT: What is the prejudice to you? I am hearing there is no prejudice, that you have been waiting this long, regrettably you have been waiting longer than I personally would have wanted you to wait, although the motions, as I see it, weren't really technically ripe until June of this year, I am being a little hard on myself. But you have been waiting based on the change of venue motion and so forth. What is the harm in waiting a few more weeks until the Court has had an opportunity to rule on the

pending motion?

MR. ZIMMERMAN: Your Honor, as we outlined in our pleadings, we believe there are three prejudices. The first is what I outlined, it is simply inequitable to allow defendants to take substantial discovery and get away with just not responding in kind, and then stay discovery.

Moreover, as your Honor stated earlier on, delay itself can be highly prejudicial. Witnesses' memories can fade, documents can be lost. At the time we opposed this we were heavily involved in third-party discovery. Stopping that process only to start it over again is prejudicial.

THE COURT: Thank you, counsel.

MR. ZIMMERMAN: Thank you.

THE COURT: Anything?

MR. QUINN: May I respond?

THE COURT: Yes, please, of course.

Mr. Quinn, from what I read in the plaintiff's opposition, they say discovery has only been one way here. It has been their responding to your requests on August 3rd for 17 logs, 20 doc requests, then on 8/17, the defendants serve 15 requests for admission, and they go on to say that on February 11, 2013, the defendants served an additional

request for documents and admissions, bringing the total to 47 requests for admissions and 33 document requests on a parallel track. The defendants also commenced discovery on third parties. That is page 2 of the opposition.

It does somewhat seem, it concerns me, that we have a situation where the FTC is responding to your request, yet the plaintiff has served one set of requests on you, on the defendants. It took defendants five months to produce any responsive documents, and to date have only produced documents related to contracts with their franchised and managed hotels, page 6 of their opposition.

There does seem to be an issue of equity here and fairness, and I am not sure, quite frankly, that we should, that the Court should condone that type of one-way discovery, if that is what is going on.

MR. QUINN: That actually is more just muddying of the water. So what the FTC has turned over and what they failed to disclose is the majority of the documents as you stated in our brief has been discovery from the third parties.

Also, the majority of our requests for admission for interrogatories have not been responded to, which we I think attached to the back of our reply

brief, in that we asked for certain things and they decided to claim a privilege, which they can, or claim that it is completely irrelevant to the case at issue.

For example, I think we asked in one what they consider to be reasonable data security practices. And they claim that is irrelevant. So to suggest that this has been one-sided, I think is not entirely true. But I just want to point out, to say something about the delay, I think your Honor had questioned, well, you know what.

I am, for example, going to focus my argument back. The idea in filing the motion to stay along with the motion to dismiss would be to focus discovery. And that is the purpose of the motion to stay. That is why we are requesting that your Honor hold discovery in abeyance, figure out what is in the case after the motion to dismiss, if there is anything and then the parties, to the extent you would, it would be -- we would take it from there.

THE COURT: Mr. Quinn, I remember my question. I asked on page 10 of the opposition, the defendant's knowledge, plaintiff says, defendants acknowledge that they have not challenged the FTC authority to bring this claim. Motion to dismiss, ECF number 32.

And it says, in parens, WHR does not dispute that FTC can bring enforcement action against companies that make deceptive statements to consumers. And so I am curious that if there is not a challenge with respect to count 1, why shouldn't we get moving on count 1? At least the discovery as it relates to the deception claim?

MR. QUINN: Because then it would just be inefficient for the purposes of the Court and the parties.

THE COURT: Chances are, right, that the Court is going to issue, by the time Judge Dickson, I am now paired with Judge Dickson, by the time Judge Dickson sets this down for a Rule 16 conference, gets the party to exchange some discovery, this Court will have ruled. Or close thereafter.

So I am just wondering whether we are delaying the inevitable as it relates to count 1.

MR. QUINN: I don't think we are, your Honor. And again, this is the motions to dismiss present threshold issues which the FTC concedes on page 10 of its brief. We are asking simply that the Court hold discovery in abeyance and let the motions play out as they will, and then we will take it from there. I mean, that is appropriate, and good cause is for that

reason, this will narrow discovery.

And one more point.

Your Honor, there is a challenge to count 1 that would also dismiss that count in its entirety. So it won't be in the parties' best interest, or the Court's best interest to bifurcate that.

THE COURT: Okay. Any response from the FTC?

MR. ZIMMERMAN: I don't want to delay in any longer. I will respond quickly. Many of the documents we produced thus far to Wyndham have been public documents because their discovery sought public statements of commissioners. Based on that, we produced it.

Moreover, their argument that they would like to focus discovery is a little late. They initially filed these motions in Arizona back in August, and they could have filed to stay discovery at that time. They chose not to. They chose to aggressively pursue discovery.

Finally, as to the discussion you had at the end, I think there is some confusion. Wyndham has claimed that good cause exists to stay the discovery because they have challenged the FTC's allegedly novel use of the unfairness here, and that should weigh in the balance in their favor of staying it. Our point

is to count 1 is that yes, they have moved to dismiss count 1, but they have not brought a challenge to the alleged novel authority.

THE COURT: They haven't challenged the authority to bring an action under count 1.

MR. ZIMMERMAN: Exactly. Thank you, your Honor.

THE COURT: Thank you.

All right. Well, as the parties know, the Court retains broad discretion in determining whether or not it makes sense to proceed with discovery while the motion to dismiss is pending. The question is not whether the FTC has demonstrated good cause, but rather what is permitted in light of the Court's heavy docket.

When I look at the arguments being forwarded by the defendants today, I recognize that they say there is good cause to stay at this point in time, it is a novel issue, it is a matter of first impression for the Court. But the end result is I do think that is a need to move this case forward. There is a need for the Court to exercise its discretion in moving these matters forward.

Neither I nor my colleagues are in the practice of staying discovery as a matter of course,

whenever a dispositive motion is pending, quite frankly. In very rare circumstances the district judges in this district, at least, stay discovery. Having been a magistrate judge for over four and a half years, and being paired with a number of our district judges, I know that I can speak from experience to say that it is rarely done in terms of a stay of discovery pending dispositive motions. In fact, the converse is true.

A stay pending a district judge's decision on a dispositive motion is an exception and not the rule in the District of New Jersey.

In light of the Court's heavy docket, dispositive motions often remain pending for months, and sometimes over a year. That is not going to happen in this case at this point in time because the parties have come in for oral argument at this point.

I am going to do my best to get an opinion issued rather quickly as to the issues raised during oral argument and in the briefs, and I will endeavor to keep my promise and get an opinion out expeditiously.

That being said, the Court is disinclined to let the parties stand by idly while memories continue to fade, and evidence becomes stale.

Moreover, experience has taught us, and me in particular, that going forward with discovery encourages amicable resolution of disputes which in turn prevents the Court from being crushed by the heavy weight of our docket.

In this particular matter, I don't necessarily think that we are going to have a resolution of this case any time soon. And in fact, it will require the Court to resolve some rather hefty, and I think intellectually challenging issues that the Court will wrestle with, and do my best to issue a thoughtful opinion in the near future.

But under the circumstances, considering, as I said when I started questioning Mr. Quinn, this case has been out there since as far back as June of last year. We have had motion practice, which I can respect, but the time has come. We are going to move forward.

So I will ask Judge Dickson to bring the parties in in the next few weeks for a Rule 16 conference, to set a schedule that the parties can follow, and I anticipate there are going to be discovery issues, and I recognize that the parties are advocates, and they are doing their jobs, but I will caution the parties to really only raise those issues

that are real issues in dispute with respect to discovery.

And I am going to keep a watchful eye on discovery in this case, and I hope to not have to intervene with discovery. But I am not going to have this case delayed based on any issues, and so if need be, I will step in on discovery issues and make calls if I have to make to make the calls. I prefer not to, but I will leave to it Judge Dickson, and his able hands to resolve any of those pending discovery disputes that I am sure you all will start thinking about from this moment forward.

Any other issues that we need to resolve at this time?

The time is now 3:18. I will gladly deal with any issues that may be pending. If not, I thank you all for your advocacy, for the arguments that have been forwarded here today, and I wish you all safe travels.

(Adjourned at 3:20 p.m.)