

1 Lisa Weintraub Schifferle (DC Bar No. 463928)
2 Kristin Krause Cohen (DC Bar No. 485946)
3 Kevin H. Moriarty (DC Bar No. 975904)
4 Katherine E. McCarron (DC Bar No. 486335)
5 John A. Krebs (MA Bar No. 633535)
6 Jonathan E. Zimmerman (MA Bar 654255)
7 Andrea V. Arias (DC Bar No. 1004270)
8 Federal Trade Commission
9 600 Pennsylvania Ave., NW Mail Stop NJ-8100
10 Washington, D.C. 20580
11 Telephone: (202) 326-2252
12 lschifferle@ftc.gov
13 kcohen@ftc.gov
14 kmoriarty@ftc.gov
15 kmccarron@ftc.gov
16 jkrebs@ftc.gov
17 jzimmerman1@ftc.gov
18 aarias@ftc.gov

19 Attorneys for Plaintiff Federal Trade Commission

20 **IN THE UNITED STATES DISTRICT COURT**
21 **FOR THE DISTRICT OF ARIZONA**

22 Federal Trade Commission,

23 Plaintiff,

24 v.

25 Wyndham Worldwide Corporation, et al.,

26 Defendants.

Case No. 2:12-cv-01365-PHX-PGR

27 **Attachment A**

28 To

Notice of Supplemental Authority

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

FEDERAL TRADE COMMISSION,

Petitioner,

v.

1:12-cv-3005-WSD

**LABMD, INC., and MICHAEL J.
DAUGHERTY,**

Respondents.

OPINION AND ORDER

This matter is before the Court on the Federal Trade Commission’s (“FTC,” “Commission,” or “Petitioner”) “Petition of the Federal Trade Commission for an Order to Enforce Civil Investigative Demands” (“Petition”) [1].

I. BACKGROUND

On January 3, 2008, the FTC issued a “Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security” (the “2008 Resolution”). (Ex. 2 to Pet. at 3).

The 2008 Resolution authorizes the use of the FTC’s compulsory process powers, for a period of five (5) years from its issuance, “[t]o determine whether

unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act [(“FTCA”)], 15 U.S.C. § 45, as amended.” (Id.).

In 2009, the FTC learned that personally-identifiable and sensitive health information belonging to consumers was publically available on peer-to-peer (“P2P”) file sharing networks. (Pet. ¶ 6). The FTC undertook a further “inquiry to determine whether disclosures of consumers’ sensitive personal information were attributable to failures to employ reasonable data security measures in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or whether they violated any other statutes or regulations enforced by the Commission.” (Id. ¶ 7). The FTC issued Civil Investigative Demands (“CIDs”), pursuant to the 2008 Resolution, to various entities to “obtain copies of electronic files that were located on P2P networks and that contain sensitive information.” (Id. ¶ 8). In response to its CIDs, the FTC obtained a spreadsheet (the “1,718 File”) that contained information about 9,000 LabMD, Inc. (“LabMD”) customers, to include names, Social Security numbers, dates of birth, and personal health insurance information. (Id.).

In 2010, after reviewing the 1,718 File and consulting with law enforcement agencies, the FTC issued a request for information to LabMD in the form of a

“voluntary access request.” (Id. ¶ 9). The voluntary access request sought information that would help the FTC determine if LabMD “had violated laws enforced by the Commission by failing to use reasonable and appropriate security measures to safeguard sensitive information.” (Id.). LabMD responded to the voluntary access request, but the FTC was dissatisfied with the scope of materials and information that were provided. (Id. ¶ 10).

On December 21, 2011, the FTC issued CIDs to LabMD and its owner and president, Michael J. Daugherty (“Daugherty,” collectively “Respondents”), to obtain information it believed it needed to complete its investigation into Respondents’ data security policies and practices. (Id. ¶¶ 10-11). The CIDs demanded that: (1) “Daugherty and one or more representatives of LabMD . . . appear and testify at investigational hearings with FTC staff;” (2) “LabMD and Mr. Daugherty . . . respond to a limited set of interrogatories;” (3) “LabMD . . . respond to a single request for documents related to its data security practices that had not already been produced to the Commission in response to the voluntary access requests;” (4) “LabMD and Mr. Daugherty . . . provide interrogatory responses and documents by January 13, 2012, and schedule the investigational hearings for January 23, 2012;” and, (5) LabMD and Daugherty “certify that they had complied with the CID requirements.” (Pet. ¶ 11; Ex. 2 to Pet.; Ex. 3 to Pet.).

Between January and June 2012, Respondents sought to limit or quash the CIDs through the administrative appeal process established by the Code of Federal Regulations and Federal Trade Commission Rules. (Pet. ¶¶ 12-15).

On June 21, 2012, Respondents' administrative remedies in challenging the CIDs were exhausted when the FTC denied Respondents' administrative petition to limit or quash the CIDs. (Id. ¶¶ 14-15).

On June 25, 2012, the FTC staff contacted Respondents to discuss their compliance with the CIDs. (Id. ¶ 16). On June 29, 2012, Respondents replied and restated their objections to the CIDs. (Id.).

On August 29, 2012, after Respondents failed to comply with the CIDs, the FTC filed its Petition in this Court seeking an order requiring Respondents to comply with CIDs issued to them on December 21, 2011, pursuant to the FTC's authority under 15 U.S.C. §§ 46, 57b-1 of the FTCA and the 2008 Resolution. (Id. at 1-4). In its Petition, the FTC alleges that the "[R]espondents' failure to comply with the CIDs greatly impedes the Commission's ongoing investigation [into breaches of consumers' sensitive personal information], and prevents the Commission from completing its investigation in a timely manner." (Id. at 9).

On September 5, 2012, the Court ordered: (i) Petitioner to serve Respondents with its Petition; (ii) required Respondents to show cause at a hearing

on September 19, 2012, regarding why the CIDs should not be enforced; and, (iii) directed Respondents to file a pleading “stating their legal and factual support for failing to comply with the FTC’s CIDs and explaining why an order should not issue from this Court requiring compliance with the CIDs.” (Order of Sept. 5, 2012, [3] at 2-3).

On September 19, 2012, after receiving briefing by the parties, the Court held the show cause hearing and heard argument from the parties. Following the hearing, the Court ordered the FTC to file a supplemental pleading addressing the following questions:

1. In a proceeding to enforce an investigative subpoena, what is the FTC required to show to meet the requirement that the subpoena is issued in an inquiry that is within the authority of the agency?
2. Does the ‘plausible’ argument standard set out in E.E.O.C. v. Kloster Cruise, Ltd., 939 F.2d 920, 922 (11th Cir. 1991) apply to FTC enforcement actions?
3. How does the FTC meet the “within the authority of the agency” standard in this case?
4. What impact, if any, does the Federal Trade Commission’s June 21, 2012, decision have on this Court’s consideration of the “within the authority of the agency” showing required in this case?
5. Did LabMD have a means of challenging the Commission’s June 21, 2012 decision that the information security investigative inquiry here is within its authority under Section

45 and, if so, does that impact the ability of LabMD to raise the issue in this enforcement proceeding?

On September 24, 2012, the FTC filed its supplemental pleading [20]. On September 28, and October 2, 2012, Respondents and the FTC filed a response and reply, respectively [21, 22].

II. DISCUSSION

A. Standard for enforcement of an administrative subpoena

“It is well-settled that the role of a district court in a proceeding to enforce an administrative subpoena is sharply limited; inquiry is appropriate only into whether the evidence sought is material and relevant to a lawful purpose of the agency.” Kloster Cruise, 939 F.2d 920, 922 (11th Cir. 1991); see also United States v. Feaster, 376 F.2d 147, 149 (5th Cir. 1967) (“In subpoena cases the Supreme Court has rejected claims that the court must satisfy itself that probable cause exists for the agency’s contention that the subject of the subpoena is covered by the statute; the only judicial inquiry to be made in enforcing an agency subpoena is whether the evidence sought is ‘plainly incompetent or irrelevant to any lawful purpose’ of the agency.”); Tobin v. Banks & Rumbaugh, 201 F.2d 223, 224 (5th Cir. 1953) (“[I]n the absence of a clear showing of unreasonableness or gross abuse of the administrative investigative function, the Courts will not interfere with an investigation ‘merely in order to render an anticipatory judgment

on the merits.”). In other words, “a subpoena enforcement proceeding is not the proper forum in which to litigate the question of coverage under a particular statute” and “[t]he agency need not make a conclusive showing of jurisdiction to justify enforcement of the subpoena.” Kloster Cruise, 939 F.2d at 922 (citations omitted).¹

Two inquiries related to the validity of a subpoena issued by a governmental agency are appropriate to be addressed in a subpoena enforcement proceeding: (1) Whether the agency makes a “plausible argument in support of its assertion of jurisdiction”; and (2) Whether the information sought by the subpoena is “plainly incompetent or irrelevant to any lawful purpose [of the FTC].” Id.; see also Ken Roberts Co., 276 F.3d at 587 (“enforcement of an agency’s investigatory subpoena will be denied only when there is ‘a patent lack of jurisdiction’ in an agency to regulate or to investigate”); United States v. Sturm, Ruger & Co., 84 F.3d 1, 5-6 (1st Cir. 1996) (citing Kloster Cruise, 939 F.2d at 923) (“As long as the agency’s assertion of authority is not obviously apocryphal, a procedurally sound subpoena

¹ “[C]ourts of appeals have consistently deferred to agency determinations of their own investigative authority, and have generally refused to entertain challenges to agency authority in proceedings to enforce compulsory process.” FTC v. Ken Roberts Co., 276 F.3d 583, 586 (D.C. Cir. 2001) (citing cases). Consistent with other courts of appeal, the Eleventh Circuit has held that “[t]he initial determination of the coverage question is left to the administrative agency seeking enforcement of the subpoena.” Kloster Cruise, 939 F.2d at 922.

must be enforced.”); EEOC v. Tire Kingdom, Inc., 80 F.3d 449, 450-51 (11th Cir. 1996); United States v. Fla. Azalea Specialists, 19 F.3d 620, 622-23 (11th Cir. 1994); Casey v. FTC, 578 F.2d 793, 799 (9th Cir. 1978) (“The district court’s role in a subpoena enforcement proceeding is strictly limited where the subpoena is attacked for lack of agency jurisdiction. The subpoena must be enforced if the information sought is ‘not plainly incompetent or irrelevant to any lawful purpose’ of the FTC.”). Thus, the Court’s inquiry at the enforcement stage is limited. The Court addresses these questions in assessing whether to grant the FTC’s request to enforce the CIDs.

1. Plausible argument that the FTC has jurisdiction to regulate data security and consumer privacy under Section 5

Section 5 does not specifically identify data security and consumer privacy as areas in which the FTC has jurisdiction to regulate. 15 U.S.C. § 45(n). Rather, courts interpret Section 5 as a statute that broadly confers authority on the FTC to investigate and regulate unfair practices that cause or are “likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” See 15 U.S.C. § 45(n); Genuine Parts Co. v. FTC, 445 F.2d 1382, 1391 (5th Cir. 1971) (FTC accorded “extreme breadth” in conducting investigations). The authority of the FTC under Section 5 to regulate unfair

practices is broadly construed by courts because it is impossible to define what constitutes unfair practices in a constantly changing and evolving economic climate. See FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 240, 244 (1972); Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988).

In determining the limits of the FTC's authority to investigate and address unfair practices regarding failures to employ reasonable data security measures, this Court is mindful that "[c]ourts have long held that consumers are injured for purposes of [Section 5 of the FTCA] not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions." FTC v. Neovi, 604 F.3d 1150, 1156-57 (9th Cir. 2010) (citing FTC v. Winsted Hosiery Co., 258 U.S. 483, 494 (1922) (holding that "[t]he honest manufacturer's business may suffer, not merely through a competitor's deceiving his direct customer, the retailer, but also through the competitor's putting into the hands of the retailer an unlawful instrument . . ."); FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 314 (1934) (holding candy retailer liable for unfair practices although manufacturer was responsible for the element of chance that made the practices unfair); Regina Corp. v. FTC, 322 F.2d 765, 768 (3d Cir. 1963) (explaining that "[w]ith respect to those instances where petitioner did not

contribute to the [misleading act], it is settled that [o]ne who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act”) (quotation marks and citations omitted).

“The statutory scheme at issue here ‘necessarily gives the Commission an influential role in interpreting section 5 and in applying it to facts of particular cases arising out of unprecedented situations.’” Orkin Exterminating Co., 849 F.2d at 1367-68 (quoting FTC v. Colgate-Palmolive, Co., 380 U.S. 374, 385 (1965)).

“Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis.” Am. Fin. Servs. Ass’n v. FTC, 767 F.2d 957, 967 (D.C. Cir. 1985); see also Orkin, 849 F.2d at 1368 (FTC’s Section 5 authority is a “broad mandate conferred upon the Commission by Congress.”); FTC v. Windward Mktg., Inc., No. Civ.A. 1:96-CV-615F, 1997 WL 33642380, at *11 (N.D. Ga. Sept. 30, 1997) (“Congress has not enacted any more particularized definition of unfairness to limit the Commission’s discretion.”).

Although it is given broad discretion to determine what constitutes an unfair practice, the FTC’s authority to investigate unfair practices using its subpoena enforcement power is not unlimited. Courts measure the validity of an FTC

subpoena against the purposes stated in the FTC resolution authorizing an investigation into specific practices. See 15 U.S.C. § 57b-1(i);² FTC v. Invention Submission Corp., 965 F.2d 1086, 1092 (D.C. Cir. 1992).

Respondents argue that the CIDs here are invalid because the 2008 Resolution was issued before the FTC learned of the existence of the 1,718 File and, in any event, is too vague to support the issuance of an administrative subpoena seeking information from LabMD. (See Ex. 2 to Pet. at 3). Respondents also assert that the FTC's claim of authority to regulate data security is not based on any threat of substantial injury to consumers, but only gross generalities.

As to Respondents' argument that the 2008 Resolution is vague and invalid, the Court disagrees. There is no dispute that the 2008 Resolution was validly issued by the Commission and the Court finds it sufficiently specifies the nature, scope, and subject matter upon which subpoenas and demands for information may

² The FTCA provides:

Notwithstanding any other provision of law, the Commission shall have no authority to issue a subpoena or make a demand for information, under authority of this subchapter or any other provision of law, unless such subpoena or demand for information is signed by a Commissioner acting pursuant to a Commission resolution. The Commission shall not delegate the power conferred by this section to sign subpoenas or demands for information to any other person.

15 U.S.C. § 57b-1(i).

be made.³ Respondent has not cited any legal authority, and the Court has found none, that invalidates an administrative agency's subpoena because it is issued based on authority in a resolution that pre-dates the identification of a specific issue of concern within the scope of that resolution. See Invention Submission Corp., 965 F.2d at 1092 (quoting FTC v. Carter, 636 F.2d 781, 789 (D.C. Cir. 1980)) (“clear that ‘the validity of Commission subpoenas is to be measured against the purposes stated in the resolution, and not by reference to extraneous evidence’”).

The Court also disagrees with Respondents' contention that there is no basis for the FTC to investigate and regulate data security and consumer privacy because there is no threat of substantial injury to consumers. The FTC presents sufficient information in its pleadings to support its claim that there is a significant and

³ The 2008 Resolution states, under a heading entitled “Nature and Scope of Investigation,” that it was adopted to permit the FTC:

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

(Ex. 2 to Pet. at 3).

widespread impact and threat to consumers, including identity theft, that results from breaches of data security and consumer privacy. (See Pet’r’s Supplemental Mem. in Supp. of Pet. to Enforce Civil Investigative Demand [20] at 9-10; Pet’r’s Reply Mem. in Supp. of Pet. [15] at 8, 12-13). The Court finds that the FTC presents a plausible argument for the exercise of its jurisdiction to investigate and enforce in the realm of data security and consumer privacy—which it has done so in at least forty-four instances since 2000—in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft—a routine occurrence in the United States. See Pl.’s Rep. in Opp’n to Wyndham Hotels and Resorts’ Mot. to Dismiss at 5, FTC v. Wyndham Worldwide Corp., Case No. 2:12-cv-01365-PHX-PGR (D. Ariz. filed June 26, 2012); Legal Resources, BCP Business Center, <http://business.ftc.gov/legal-resources/29/35> (last visited Nov. 16, 2012) (citing enforcement actions); (Pet’r’s Supplemental Mem. in Supp. of Pet. to Enforce Civil Investigative Demand at 9-10; Pet’r’s Reply Mem. in Supp. of Pet. at 8, 12-13).

The Court also finds support for the conclusion that the FTC’s argument is plausible regarding its jurisdiction because federal courts have recognized the FTC’s authority under Section 5 to investigate and use its authority to address unfair practices regarding related data security and consumer privacy issues. See

FTC v. Pricewert, LLC, No. C-09-2407 RMW, 2010 WL 329913, at *2-*3 (N.D. Cal. 2010) (Section 5 used to address “distribution of illegal, malicious and harmful electronic content”); FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009) (Section 5 used to address marketing of a software program that could be used illegitimately to commit identity theft); FTC v. Accusearch, Inc., No. 06-CV-105-D, 2007 WL 4356786, at *1, *7-*8 (D. Wyo. Sept. 28, 2007), aff’d 570 F.3d 1187 (10th Cir. 2009) (Section 5 used to address the unauthorized disclosure of confidential customer phone records); FTC v. Seismic Entm’t Prods., Inc., No. Civ. 04-377-JD, 2004 WL 2403124, at *2-*4 (D.N.H. 2004) (Section 5 used to address internet advertising methods that cause unauthorized changes to computers and that affect data security).

Although the Court finds there is significant merit to Respondents’ argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues, it is a plausible argument to assert that poor data security and consumer privacy practices facilitate and contribute to predictable and substantial harm to consumers in violation of Section 5 because it is disturbingly commonplace for people to wrongfully exploit poor data security and consumer privacy practices to wrongfully acquire and exploit personal consumer

information. Because the FTC's assertion of jurisdiction to issue its CIDs is premised on a plausible argument, the Court finds that Respondents' argument that the CIDs should not be enforced for a lack of jurisdiction is not a sufficient reason to deny the FTC's request for enforcement. See Kloster Cruise, 939 F.2d at 922.

2. *Whether the information sought by the subpoena is unreasonable or "plainly incompetent or irrelevant to any lawful purpose [of the FTC]"*

With regard to administrative subpoenas issued by the FTC, the Supreme Court has stated:

Even if one were to regard [a] request for information . . . as caused by nothing more than official curiosity, nevertheless lawenforcing [sic] agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest.

Of course a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power. Federal Trade Comm. v. American Tobacco Co., supra. But it is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant. 'The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.' Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 208, 66 S.Ct. 494, 505, 90 L.Ed. 614, 166 A.L.R. 531.

See United States v. Morton Salt Co., 338 U.S. 632, 652-53 (1950).

Thus, “[t]he chief limitation on an investigation by an administrative agency is that it must meet the test of reasonableness.” Genuine Parts Co., 445 F.2d at 1391 (citing Oklahoma Press Publishing Co. v. Walling, 327 U.S. at 208). The information sought by the FTC also must “not [be] plainly incompetent or irrelevant to any lawful purpose.” See Kloster Cruise, 939 F.2d at 922 (quotations omitted). In seeking information in an investigation, the FTC is accorded “extreme breadth” by courts when evaluating its demands for testimony and documents. See Genuine Parts Co., 445 F.2d at 1391.

Furthermore, the burden of showing that an administrative subpoena is unreasonable is a heavy one because

[s]ome burden on subpoenaed parties is to be expected and is necessary in furtherance of the agency’s legitimate inquiry and the public interest. The burden of showing that the request is unreasonable is on the subpoenaed party. Further, that burden is not easily met where . . . the agency inquiry is pursuant to a lawful purpose and the requested documents are relevant to that purpose. Broadness alone is not sufficient justification to refuse enforcement of a subpoena. Thus courts have refused to modify investigative subpoenas unless compliance threatens to unduly disrupt or seriously hinder normal operations of a business.

See FTC v. Texaco, Inc., 555 F.2d 862, 882 (D.C. Cir. 1977).

The FTC here demands documents and testimony related to the public disclosure on P2P networks of Respondents’ 1,718 File containing the names and

sensitive information of 9,000 consumers and LabMD's data security practices. The Court has reviewed the FTC's CIDs in this action and finds they are specific in scope, reasonably relevant to its investigation into LabMD's data security practices, and, even though LabMD has already produced a significant amount of material, are not duplicative or unreasonable. (See Ex. 2 to Pet. at 11-12; Ex. 3 to Pet. at 8). The Court finds that the demands in the CIDs—beyond being based on a plausible argument regarding the FTC's statutory authority and jurisdiction—are not too indefinite and the information sought is reasonably relevant to its investigation into Respondents' data security and customer privacy practices.

In light of the “sharply limited” “role of a district court in a proceeding to enforce an administrative subpoena,” the Court finds the CIDs are required to be enforced because there is a plausible argument for the exercise of jurisdiction by the FTC and “the evidence sought is material and relevant to a lawful purpose of the agency.” See Kloster Cruise, 939 F.2d at 922.

III. CONCLUSION


For the foregoing reasons,

IT IS HEREBY ORDERED that Petitioner's Petition [1] is **GRANTED**.

IT IS FURTHER ORDERED that, no later than December 15, 2012,

Respondents shall comply with Petitioner's Civil Investigative Demands.

SO ORDERED this 26th day of November, 2012.



WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE