UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

Office of the Secretary

April 20, 2012

VIA E-MAIL AND COURIER DELIVERY

Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP
2900 K Street, N.W.
North Tower - Suite 200
Washington, D.C. 20007
E-mail: claudia.callaway@kattenlaw.com

RE: *LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand*; and *Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand*

Dear Ms. Callaway, Ms. Grigorian, and Mr. Dayal:

On January 10, 2012, the Federal Trade Commission ("FTC" or "Commission") received the above Petitions filed by LabMD, Inc. ("LabMD") and its President, Michael J. Daugherty (collectively, "Petitioners"). This letter advises you of the Commission's disposition of the Petitions, effected through this ruling by Commissioner Julie Brill, acting as the Commission's delegate.[1]

For the reasons explained below, the Petitions are denied. You may request review of this ruling by the full Commission.[2] Any such request must be filed with the Secretary of the Commission within three days after service of this letter ruling.[3] The timely filing

[1] *See* 16 C.F.R. § 2.7(d)(4).

[2] 16 C.F.R. § 2.7(f).

[3] *Id.* This ruling is being delivered by e-mail and courier delivery. The e-mail copy is provided as a courtesy, and the deadline by which an appeal to the full Commission

of a request for review by the full Commission shall not stay the return dates established by this ruling.[4]

I. INTRODUCTION

The FTC commenced its investigation into the adequacy of LabMD's information security practices in January 2010, after a LabMD file had been discovered on a peer-to-peer ("P2P") file sharing network.[5] The file, which Petitioners call the "1,718 File" because it is 1,718 pages long, is a spreadsheet of health insurance billing information for uropathology and microbiology medical tests of around 9,000 patients. It contains highly sensitive information about these consumers, including:

- Name;
- Social Security Number;
- Date of birth;
- Health insurance provider and policy number; and
- Standardized medical treatment codes.[6]

Such information can be misused to harm consumers.

The purpose of the investigation is to determine whether Petitioners violated the FTC Act by engaging in deceptive or unfair acts or practices relating to privacy or information security. The inquiry is authorized by Resolution File No. P954807, which provides for the use of compulsory process in investigations of potential Section 5 violations involving "consumer privacy and/or data security."

---

would have to be filed should be calculated from the date on which you receive the original letter by courier delivery.

[4] *Id.*

[5] P2P programs allow users to form networks with others using the same or a compatible P2P program. Such programs allow users to locate and retrieve files of interest to them that are stored on computers of other users on the networks.

[6] LabMD Pet., Ex. C, at Fig. 4. Because the LabMD and Daugherty Petitions make the same arguments (the Petitions differ only in details about the submitter), we generally cite only to LabMD's Petition.

The investigation began with voluntary information requests for documents and information about LabMD's information security policies, procedures, practices, and training generally, as well as information about security incidents, including, but not limited to, the discovery of the 1,718 File on P2P networks. In response, LabMD produced hundreds of pages of documents, including supplements and responses to follow-up questions. To complete the investigation, staff requested issuance of CIDs to LabMD and Michael J. Daugherty, LabMD's President.

The Commission issued the CIDs on December 21, 2011. Both require testimony relating to information security policies, practices, training, and procedures. They also include a limited number of interrogatories that require Petitioners to identify documents used by the witnesses to prepare for their testimony.[7] The LabMD CID also includes a single document request asking for only those documents that were both identified in response to the CID's interrogatories and had not been previously produced to staff.[8]

Petitioners seek to quash or limit the CIDs because, they claim, the CIDs "appear to be premised on" the download of the 1,718 File (hereinafter, the "File disclosure").[9] Their principal objection relates to the merits of the investigation. In particular, they contend (without citing any authority) that the Commission must have a "justifiable" belief that a law violation has occurred before it can issue CIDs, and that the File disclosure cannot support such a belief. They claim that the File disclosure occurred not because LabMD failed to implement reasonable and appropriate security measures, but because the company was the victim of an illegal intrusion conducted by Tiversa (a P2P information technology and investigation services company) and Dartmouth College faculty using Tiversa's powerful P2P searching technology.[10] Further, Petitioners argue that no actual harm to consumers resulted from the File disclosure.[11] Accordingly, they

[7] LabMD Pet., Ex. A.

[8] LabMD Pet., Ex. A.

[9] LabMD Pet., at 1.

[10] Petitioners claim that in the course of a Department of Homeland Security-funded research project, Professor M. Eric Johnson of Dartmouth College's Tuck School of Business and Tiversa used Tiversa's P2P searching technology to search for and then download the file. LabMD Pet., at 3-4, 7, & Ex. F, at 10-12.

[11] The Petitions claim that there is no allegation of actual consumer injury from the File disclosure. LabMD Pet., at 7.

contend that investigating either the File disclosure or the adequacy of LabMD's security practices is improper because no law violation can have occurred, and that the CIDs therefore should be quashed.[12]

As discussed below, these arguments are undermined by: (1) the obvious point that an investigation necessarily must precede assessment of whether there is reason to believe a law violation may have occurred (in any matter); (2) the scope of the authorizing resolution; and (3) the language of the FTC Act. The resolution authorizes use of compulsory process in an investigation to determine whether Petitioners engaged in deceptive or unfair practices related to privacy or security. Petitioners' focus on the File disclosure is misplaced – it may bear on the adequacy of LabMD's security practices under the FTC Act but does not establish the investigation's scope under the resolution.[13] Further, in such an investigation Section 5 directs the Commission to consider whether security practices are unfair because they create a sufficient risk of harm, even if no harm has been reported.

Petitioners make two additional arguments in support of their Petitions. First, they argue that the resolution authorizing the CIDs did not provide them with sufficient notice of the purpose and scope of the investigation. Second, they argue that the FTC is without jurisdiction to pursue this investigation. Both of these additional arguments are equally without merit.

II. ANALYSIS

A. The applicable legal standards.

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as that inquiry is defined by the investigatory resolution.[14]

---

[12] LabMD Pet., at 7-8.

[13] *See, e.g.*, *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008) (confirming that the scope of an investigation authorized by Resolution P954807 properly included all of CVS' "consumer privacy and data security practices" (including its computer security practices) and could not be limited (as the company argued) to just known incidents of unauthorized disposal of paper documents in dumpsters).

[14] *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have "a justifiable belief that wrongdoing has actually occurred," as Petitioners claim.[15] As the D.C. Circuit has stated, "The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one . . . . The requested material, therefore, need only be relevant to the *investigation* – the boundary of which may be defined quite generally, as it was in the Commission's resolution here."[16] Agencies thus have "extreme breadth" in conducting their investigations,[17] and "in light of [this] broad deference . . ., it is essentially the respondent's burden to show that the information is irrelevant."[18]

B. The CIDs satisfy the foregoing standards.

Petitioners argue that the CIDs are improper for several reasons. In particular, they claim no law violation could have occurred, by arguing that: (1) not even "perfect" security measures (let alone the reasonable security measure standard the Commission uses to determine whether a law violation may have occurred) could have prevented the File disclosure because Tiversa's technology "can penetrate even the most robust network security,"[19] and (2) no actual injury resulted from the File disclosure.

---

[15] LabMD Pet., at 6. *See, e.g.*, *Morton Salt*, 338 U.S. at 642-43 ("[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.").

[16] *Invention Submission*, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing *FTC v. Carter*, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

[17] *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1517 (D.C. Cir. 1993) (citing *Texaco*, 555 F.2d at 882).

[18] *Invention Submission*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) ("burden of showing that the request is unreasonable is on the subpoenaed party"). *Accord FTC v. Church & Dwight Co.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010).

[19] LabMD Pet., at 7.

The Commission is not required, as a precondition to conducting a law enforcement investigation, to make a showing that it is likely that a law violation has occurred. The D.C. Circuit confirmed this point in *FTC v. Texaco, Inc.*, when it stated, "[I]n the pre-complaint stage, an investigating agency is under no obligation to propound a narrowly focused theory of a possible future case . . . . The court must not lose sight of the fact that the agency is merely exercising its legitimate right to determine the facts, and that a complaint may not, and need not, ever issue."[20] Here, Petitioners seek to quash the CIDs by asserting that LabMD's practices must have been reasonable under the FTC Act because the 1,718 File was retrieved using Tiversa's powerful searching technology. Accepting this argument would prevent the Commission from exploring relevant issues bearing on reasonableness, such as, for example, whether the company's security practices could have prevented the 1,718 File from being retrieved using the common P2P programs that are used by millions of computer users each day or whether there were readily available security measures LabMD did not implement that would have prevented even Tiversa's technology from successfully retrieving the file. Although such evidence (if it exists at all) could undermine their reasonableness claim, Petitioners nonetheless argue that the Commission cannot use CIDs to investigate whether the evidence exists unless it already has reason to believe it does exist. For this reason, Petitioners' argument that the strength of Tiversa's P2P searching technology precludes the possibility that a law violation occurred, regardless of the state of LabMD's security, must fail.

Similarly, Petitioners' assertion that no law violation can have occurred because no actual harm has been shown also fails because, under Section 5, a failure to implement reasonable security measures may be an unfair act or practice if the failure is *likely* to cause harm. No showing of actual harm is needed.[21]

Both arguments conflate the purpose of a CID with the purpose of a future potential complaint. A CID can only compel information necessary for an investigation, and the investigation may or may not result in allegations of a law violation.[22]

---

[20] 555 F.2d 862, 874 (D.C. Cir. 1977). This holding from *Texaco* has been repeatedly reaffirmed, most recently in *FTC v. Church & Dwight*, 747 F. Supp. 2d 3, 6, *aff'd*, 2011 U.S. App. LEXIS 24587 (D.C. Cir. Dec. 13, 2011).

[21] 15 U.S.C. § 45(n) (an unfair practice is one that "causes or *is likely to cause* substantial injury to consumers"); *see also* FTC Policy Statement on Unfairness, 104 F.T.C. 949, 1073 & n.15 (1984).

[22] Petitioners also argue that the CIDs are improper for other reasons. They claim that because security issues posed by P2P programs were common (according to Tiversa), such issues could not constitute an unfair or deceptive practice in violation of the FTC

Additionally, Petitioners have claimed that the CIDs are burdensome, but they have not come forward with any support for these assertions. Instead, they make only bald statements that the CIDs are "highly burdensome," "unduly burdensome," "costly and burdensome," and "deeply burdensome."[23] Having offered no factual information about the alleged burdens of complying with the CIDs, Petitioners have not sustained their burden to demonstrate that the CIDs are unduly burdensome.[24]

Such a showing would be difficult here in any event. Notwithstanding Petitioners' description, the CIDs call primarily for testimony, not documents. Thus, it seems unlikely that compliance would require large-scale or time-consuming document production.

Act. LabMD Pet., at 7-8 & n.34. This argument is unavailing. The fact that a particular practice may be pervasive or widespread has no bearing on whether the FTC may investigate it as also deceptive or unfair. Indeed, accepting Petitioners' argument would confine the FTC to investigating only those activities that were rare or uncommon, thus crippling the agency's law enforcement mission. Along the same lines, Petitioners contend that the risks of P2P technology, and the resulting potential liabilities to businesses, were not known in 2008, when the File disclosure occurred. In support of this claim, they assert that the FTC did not notify businesses or publish guidance about P2P until 2010. LabMD Pet., at 8. In fact, many, including the FTC, warned about the risks presented by P2P programs years before the File disclosure occurred. *See, e.g.*, FTC Staff Report, "Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues" (June 2005), available at http://www.ftc.gov/reports/ p2p05/050623p2prpt.pdf; Prepared Statement of the Federal Trade Commission Before The Committee on Oversight and Government Reform, United States House of Representatives (July 24, 2007) (discussing P2P programs and risks), available at http://www.ftc.gov/os/testimony/P034517p2pshare.pdf.

[23] LabMD Pet., at 7, 9, & 10.

[24] *See, e.g.*, *Texaco*, 555 F.2d at 882 ("The burden of showing that the request is unreasonable is on the subpoenaed party.") (citing *United States v. Powell*, 379 U.S. 48, 58 (1964)); *accord EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986) (subpoena is enforceable absent a showing by recipient that the requests are unduly burdensome); *FTC v. Standard American, Inc.*, 306 F.2d 231, 235 (3d Cir. 1962) (recipient has responsibility to show burden and must make "a record . . . of the measure of their grievance rather than ask [the court] to assume it"); *In re Nat'l Claims Serv., Inc.*, 125 F.T.C. 1325, 1328-29 (1998) (FTC ruling that petition to quash must substantiate burden with specific factual detail).

Furthermore, to the extent that the CIDs call for narrative responses, they merely require Petitioners to identify documents related to the requested testimony. In fact, there is only one specification that requires the production of documents, and even that specification is limited to documents identified in response to the interrogatories to the extent they were "not already been produced to the FTC."[25]

Finally, Petitioners, without explaining its relevance, contend that the timing of the CIDs is "troubling," coming after LabMD's conduct had been reviewed by two congressional committees, and after LabMD filed suit against Tiversa and others alleging conversion and trespass, among other violations, based on the File disclosure in 2008.[26] Though Petitioners seem to believe that there is some connection between their rejection of Tiversa's offer to provide LabMD with information security services, their subsequent lawsuit, and the FTC's investigation, the chronology of the investigation does not support such a conclusion. The FTC first contacted LabMD for information in January 2010, well before LabMD filed its lawsuit against Tiversa in October 2011.[27] Moreover, the claim that LabMD's conduct was reviewed by congressional committees does not appear to be based on evidence presented in the Petitions. Although Petitioners have attached as exhibits three instances of congressional testimony by Tiversa, none identifies LabMD by name or discusses the specifics of the File disclosure.

C. The resolution provides sufficient notice of the purpose and scope of the FTC's investigation.

Under the FTC Act, a CID is proper when it "state[s] the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation."[28] It is well-established that the resolution authorizing the process provides the requisite statement of the purpose and scope of the investigation,[29]

---

[25] LabMD Pet., Ex. A.

[26] LabMD Pet., at 9 & Ex. F.

[27] We note further that this suit came more than three years after the solicitations Petitioners complain of in their Petitions. LabMD Pet., Ex. F, at 1, 17-23.

[28] 15 U.S.C. § 57b-1(c)(2).

[29] *Invention Submission.*, 965 F.2d at 1088; *accord Texaco*, 555 F.2d at 874; *FTC v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980); *FTC v. Anderson*, 631 F.2d 741, 746 (D.C. Cir. 1979).

and also that the resolution may define the investigation generally, need not state the purpose with specificity, and need not tie it to any particular theory of violation.[30]

Despite this, Petitioners object that Resolution File No. P954807 did not provide sufficient notice of the purpose and scope of the investigation, and they further claim that this resolution is inadequate under the standard developed by the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980).[31]

Petitioners' first argument reads the governing standard too narrowly. Resolution File No. P954807 authorizes the use of compulsory process:

> to determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended.[32]

This general statement of the purpose and scope of the investigation is more than sufficient under the standard for such resolutions, and courts have enforced compulsory process issued under similarly broad resolutions.[33]

Petitioners' reliance on *Carter* is also misplaced. While *Carter* held that a bare reference to Section 5, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue in that case, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further

---

[30] *Invention Submission*, 965 F.2d at 1090; *Texaco*, 555 F.2d at 874 & n.26; *FTC v. Nat'l Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (citing *EPA v. Alyeska Pipeline Serv. Co.*, 836 F.2d 443, 477 (9th Cir. 1988)).

[31] LabMD Pet., at 10-12.

[32] LabMD Pet., Ex. A.

[33] *See FTC v. Nat'l Claims Serv.*, 1999 WL 819640, at *2 (finding omnibus resolution referring to FTC Act and Fair Credit Reporting Act sufficient); *FTC v. O'Connell Assoc., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution). The Commission has repeatedly rejected similar arguments about such omnibus resolutions. *See, e.g.*, *Firefighters Charitable Found.*, No. 102-3023, at 4 (Sept. 23, 2010); *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

related it to the subject matter of the investigation.[34] With this additional information, the Court felt "comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit . . . ."[35]

The resolution here, like the one in *Carter*, does not cite solely to Section 5, but also recites the subject matter of the investigation: "deceptive or unfair acts or practices related to consumer privacy and/or data security." Since the resolution here discloses the subject matter of the investigation in addition to invoking Section 5, the resolution provides notice sufficient under *Carter* of the purpose and scope of the investigation.

As a final note, the history of the investigation itself undermines Petitioners' argument that the present CIDs do not sufficiently advise them of the nature and scope of the investigation. Petitioners have been under investigation since January 2010 and have engaged in repeated discussions with staff. At no point have Petitioners indicated they did not understand the purpose or scope; in fact, Petitioners have already produced hundreds of pages of documents in response to staff requests. Moreover, the Petitions under consideration here present highly detailed and factual arguments going to the very merits of the investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners.[36]

D. Petitioners' challenge to the FTC's regulatory authority is premature and without basis.

Petitioners' final argument is that the FTC lacks jurisdiction to conduct the instant investigation.[37] Petitioners assert that LabMD is a health care company and that the

---

[34] *Carter*, 636 F.2d at 788.

[35] *Id.*

[36] *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) ("[T]he notice provided in the compulsory process resolutions, CIDs and other communications with Petitioner more than meets the Commission's obligation of providing notice of the conduct and the potential statutory violations under investigation.").

[37] Petitioners also claim that the resolution does not meet the requirements established by the FTC's Operating Manual. LabMD Pet., at 10. As discussed above, by disclosing the statutory basis and subject matter of the investigation, the resolution does provide notice as required by the Operating Manual. That said, the Operating Manual, by its own terms, is advisory. It is not a "basis for nullifying any action of the Commission or the staff."

information disclosed in the 1,718 File is protected health information ("PHI") under the Health Insurance Portability and Accountability Act ("HIPAA"). Accordingly, they contend, the adequacy of their security practices with respect to this information is subject to the exclusive jurisdiction of HHS.[38]

As an initial matter, it is well-established that challenges to the FTC's jurisdiction are not properly raised through challenges to investigatory process. As the D.C. Circuit stated: "Following *Endicott* [*Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (1943)], courts 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."[39] The reasons for such a rule are obvious. If a party under investigation could raise substantive challenges in an enforcement proceeding, before the agency has obtained the information necessary for its case – essentially requiring the FTC to litigate an issue before it can learn about it – then the FTC's investigations would be foreclosed or substantially delayed.[40] Thus, Petitioners' basic challenge to the FTC's jurisdiction is premature and will not support quashing the instant CIDs.

In any event, the claim that HHS has exclusive jurisdiction to investigate privacy and data security issues involving PHI is without basis. Petitioners essentially invoke the doctrine of implied repeal to assert that HIPAA and its Privacy and Security Rules displace FTC jurisdiction. But implied repeal is "strongly disfavored," for two reasons.[41] First, courts have recognized that agencies may have overlapping or concurrent jurisdiction, and thus that the same issues may be addressed and the same parties

---

Operating Manual, § 1.1.1.1. *See also FTC v. Nat'l Bus. Consultants, Inc.* 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶68,984, at *29 (E.D. La. March 19, 1990).

[38] LabMD Pet., at 12-13.

[39] *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (citing *United States v. Sturm, Ruger & Co.*, 84 F.3d 1, 5 (1st Cir. 1996)); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 468-73 (2d Cir. 1996); *EEOC v. Peat, Marwick, Mitchell & Co.*, 775 F.2d 928, 930 (8th Cir. 1985); *Donovan v. Shaw*, 668 F.2d 985, 989 (8th Cir. 1982); *FTC v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979); *accord Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 213-14 (1946).

[40] *Texaco*, 555 F.2d at 879.

[41] *Galliano v. United States Postal Serv.*, 836 F.2d 1362, 1369 (D.C. Cir. 1988).

proceeded against simultaneously by more than one agency.[42] Second, courts rarely hold that one federal statute impliedly repeals another because "'when two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective.'"[43] Thus, repeals by implication will only be found where the Congressional intent to effect such a repeal is "clear and manifest."[44]

Petitioners can point to no such "clear or manifest" evidence that Congress intended HIPAA or its rules to displace the FTC Act. The authority Petitioners cite for the proposition that HHS has exclusive jurisdiction does not address such repeal.[45] To the contrary, there is ample evidence against such implied repeal. For one, the same authority cited by Petitioners – the preamble to the Privacy Rule – expressly provides that entities covered by that Rule are "also subject to other federal statutes and regulations."[46] Also, this preamble includes an "Implied Repeal Analysis," which is silent as to any implied repeal of the FTC Act.[47] Recent legislation shows that, if anything, Congress intended the FTC and HHS to work collaboratively to address potential privacy and data security risks related to health information. The American Recovery and Reinvestment Act of 2009, for instance, required HHS and the FTC to develop harmonized rules for data breach notifications by HIPAA-covered and non-HIPAA-covered entities, respectively. *See* 74

---

[42] *FTC v. Cement Inst.*, 333 U.S. 683, 694 (1948); *see also Texaco*, 555 F.2d at 881 ("[T]his is an era of overlapping agency jurisdiction under different statutory mandates."); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986). Because agencies have overlapping jurisdiction, they often work together. For instance, the FTC and HHS collaborated on the investigation of CVS Caremark Corporation. *See CVS Caremark Corp.*, No. 072-3119, at 7 (Aug. 6, 2008).

[43] *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976) (quoting *Morton v. Mancari*, 417 U.S. 535, 551 (1974)).

[44] *Id.* at 154.

[45] LabMD Pet., at 12 (citing 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000)). This Federal Register notice is the Notice of Public Rulemaking for the Privacy and Security Rules under HIPAA. The excerpt cited by Petitioners does not address the scope of HHS' enforcement jurisdiction, but rather discusses the delegation of enforcement authority from the Secretary of HHS to HHS' Office for Civil Rights. 65 Fed. Reg. 82,472 (Dec. 28, 2000).

[46] 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000).

[47] *Id.* at 82,481-487.

Fed. Reg. 42,962, 42,962-63 (Aug. 25, 2009). Thus, HIPAA and its Rules do not serve to repeal FTC jurisdiction, which is overlapping and concurrent to HHS'.

This is particularly appropriate where, as here, the consumer information at issue included more than just health information. The consumer information exposed in the 1,718 File also included names, Social Security numbers, and dates of birth. While this information can be considered PHI under HIPAA when combined with health information, the information clearly exposes consumers to the risk of identity theft and is exactly the kind of sensitive personal information that the Commission is charged with protecting under Section 5 of the FTC Act and other statutes. Petitioners have provided no proper basis to challenge the investigation as an exercise of the Commission's jurisdiction under these authorities.

III. CONCLUSION AND ORDER

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6); and

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must now be produced on or before May 11, 2012.

By direction of the Commission.

Donald S. Clark
Secretary