containers located behind CVS pharmacies in Indianapolis, IN between June and September 2006. *Id*. at 5. Additionally, between September 2006 and May 2007, additional media reports indicated that sensitive consumer information was found in the trash containers behind CVS pharmacies in Indiana, Ohio, Kentucky, Arizona, and Texas.[2] *Id*. at 8.[3] By letter dated September 27, 2007, FTC staff advised CVS that the Commission was conducting an inquiry "to determine whether CVS's handling of sensitive information from or about its consumers in connection with the preparation and sale of prescription medicines and supplies raises any issues under Section 5." *Id*. at 5 (quoting from Exhibit C to the Petition at 1-2 [Letter from Alain Sheer, FTC Div. of Privacy and Identity Protection, to Christine L. Egan, Esquire, Asst. Gen. Counsel, for CVS]). That letter further asked CVS to voluntarily provide information identified in the letter to the FTC and/or HHS for their use in their coordinated investigations. Petition, Exh. C at 2-8. Paragraph 9 of the specification in the letter included "documents sufficient to identify all policies and statements made by CVS regarding its collection, disclosure, use, and protection of personal information. . . ." *Id*. at 4. CVS claims that it cooperated with the FTC's investigation, and voluntarily "provided information and voluminous documents relevant to the inquiry. . . ."[4] Petition at 2.

---

[2] CVS has over 6,000 retail pharmacies, *compare* Petition at 5 ("over 6,200") *with* Petition at 7 ("now more than 6300"), in forty (40) states and the District of Columbia, and has more than 190,000 employees in its retail pharmacy operations. Petition at 5.

[3] CVS refers to these reports collectively as the "Dumpster Incidents." Petition at 7. For the sake of convenience, the FTC will use this same phrase to refer to these events. In addition, a June, 2005 *Computerworld* article reported a potential security vulnerability in the CVS ExtraCare FSA program. *Id.* at 9-10. ExtraCare is the name CVS uses for its loyalty card program. *See id.* at 9. CVS indicates that its own investigation revealed no disclosure of personally identifiable information as a result of this vulnerability. *Id*. at 10.

[4] Exhibit E to the Petition (letter of December 14, 2007, from FTC Attorney Loretta Garrison to Anthony DiResta) indicates that Commission staff did not believe CVS had fully responded to its information requests.

Responses to Petitions to Quash

On May 22, 2008, CVS received the CID, issued on May 20, 2008, that is the subject of the Petition. According to CVS, the specifications of the CID seek "a massive volume of documents and information regarding the security and confidentiality of CVS's electronically stored, transmitted or accessible information that is not limited, or related at all, to: (1) the dumpster incidents or (2) the protection of the ExtraCare program information." Petition at 3-4. CVS timely fied its Petition on June 20, 2008. The Petition seeks relief from the CID on the following grounds:

> (1) CID Specifications for Documents Nos. 5, 6, and 7 and for Interrogatories Nos. 1, 6 and 7 broadly demand disclosure of vast amounts of CVS's electronically stored, transmitted or accessible information, dating back three to five years, that is not relevant to the purpose of the inquiry and is therefore unreasonable;
>
> (2) based on the overly broad definition of "Company" included in the CID, the Staff unreasonably demands documents and information, not only from CVS's retail pharmacy operations, but also from its Caremark segment, a Pharmacy Benefit Management company ("PBM") that merged with CVS in March of 2007, that remains a separate business distinct from CVS's retail pharmacy, and that had no role in the incidents that form the basis of the inquiry, all of which occurred nearly two years before the 2007 merger;
>
> (3) the challenged Specifications unreasonably demand documents and information from CVS (and its Caremark segment) which is primarily regulated by other federal agencies with exclusive administration and enforcement authority over patient privacy and security issues;
>
> (4) the CID is defective and unenforceable because the challenged Specifications demand documents and information outside the scope and purpose of the inquiry in violation of the FTC's own rules; and

> (5) compliance with the overly-broad CID Specifications in question would be unduly burdensome to CVS, not only as a result of the sheer volume of the electronically-stored, transmitted or accessible information demanded, but also because the CID further requires that CVS first redact all "Personal Information" from all such information and documents.

Petition at 4 (footnote omitted).

The gravamen of CVS's claims stems from CVS's misimpression as to the actual scope of the Commission's inquiry. CVS correctly notes that the Commission initiated its investigation because media reports indicated that CVS store personnel in several different states had disposed of sensitive consumer information by placing it in publicly-accessible trash containers – the dumpster incidents. *Id*. at 5. CVS also concedes that the Commission's investigation was directed toward a reported security vulnerability in its ExtraCare program. CVS relies on these two identified data security problems to support its claims that the FTC can only investigate issues related to the physical disposal of records at its pharmacies (the dumpster incidents) or to its ExtraCare program. *Id*. at 10-11.

In particular, CVS complains that the CID seeks information beyond the scope of the investigation, that is, "documents and information regarding the security and confidentiality of CVS'[s] electronically-stored, transmitted or electronically-accessible information that is not relevant, or related at all, to the inquiry concerning: (1) CVS'[s] practices in handling consumers' personal information with the dumpster incidents and (2) the ExtraCare program." *Id.* The security vulnerability identified in the media reports relating to the ExtraCare program involved electronically-stored, -transmitted or -accessible information. Petition at 9-10. Accordingly, CVS cannot complain that such information is, in and of itself, beyond the scope of the investigation. It must, therefore, be claiming that the investigation cannot be any broader than the precise episodes that provided the

lead information for the investigation. Put another way, the scope of the FTC's investigatory powers is, according to CVS, limited to those things the FTC knows about and excludes those things about which the FTC might be suspicious, based on the things it knows. CVS cites no authority for this position; indeed, the *Morton Salt* case that it does cite, Petition at 14, flatly contradicts CVS's position. *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950) ("[The FTC's power of inquiry] 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 assurance that it is not.").

CVS concedes that the dumpster incidents were the result of store personnel at a number of its stores around the country failing to properly adhere to CVS's own data security policies – the "Blue Bag Policy" – regarding the proper disposal of sensitive customer information.[5] Petition at 7. In sum, the dumpster incidents suggest that some areas of CVS's business operations might be affected by a degree of laxity with respect to adequate data security practices. Accordingly, the scope of the FTC's investigation is directed toward the possibility that portions of the nation's "largest provider of prescriptions and related health care services," *Id.* at 5, may have data security practices that place its customers' data in jeopardy. The Commission believes that determining the nature, scope, and, if appropriate, remediation of such risks is in the public interest.

Before turning to the issues raised by CVS in its Petition, however, it is appropriate to emphasize the fact that the party who

[5] Exhibit O [Memorandum of Apr. 7, 2008, from CVS Counsel to FTC Counsel] to the Petition describes the Blue Bag Program as a protocol for the segregation and secure disposal of sensitive waste by pharmacy personnel. In essence, sensitive customer information was to be segregated in blue bags and retained in the stores for later pick-up and disposal; in contrast, nonsensitive waste could be disposed of in the trash receptacle located outside of each store. Exhibit O at 2-5.

moves to limit the enforcement of a CID bears the burden of demonstrating that a particular CID specification is unreasonable. "[T]he burden of showing that an agency subpoena is unreasonable remains with the respondent, . . . and where, as here, the agency inquiry is authorized by law and the materials sought are relevant to the inquiry, that burden is not easily met. [citations omitted]." *Fed. Trade Comm'n v. Rockefeller*, 591 F.2d 182, 190 (2nd Cir. 1979), quoting *Sec. and Exchange Comm'n v. Brigadoon Scotch Distributing Co.,* 480 F.2d 1047, 1056 (2nd Cir. 1973), *cert. denied*, 415 U.S. 915 (1974).

II. CVS Has Not Shown that the CID Seeks Information that Is Irrelevant to the Investigation.

The scope of this investigation is determined by the terms of the resolution authorizing the use of CIDs and other compulsory process to conduct the investigation. *Fed. Trade Comm'n v. Invention Submission Corp*., 965 F.2d 1086,1091-92 (1992) ("The Commission's compulsory process resolution did not restrict the investigation to possible oral misrepresentations, however, and we have previously made 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.'") (quoting *Fed. Trade Comm'n v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980)). As the *Invention Submission* court also noted:

> It is well established that a district court must enforce a federal agency's investigative subpoena if the information sought is "'reasonably relevant,'" *FTC v. Texaco, Inc*., 555 F.2d 862, 872, 873 n. 23 (D.C. Cir.) (en banc) (quoting *United States v. Morton Salt Co.*, 338 U.S. 632, 652. . . (1950)), *cert. denied*, 431 U.S. 974. . . (1977) – or, put differently, "'not plainly incompetent or irrelevant to any lawful purpose' of the [agency]," *id*. at 872 (quoting *Endicott Johnson Corp. v. Perkins*, 317 U.S. 501, 509 . . . (1943)); *accord*

> *United States v. Aero Mayflower Transit Co.*, 83l F.2d 1142, 1145 (D.C. Cir. 1987) – and not "unduly burdensome" to produce, *Texaco*, 555 F.2d at 881. We have said that the agency's own appraisal of relevancy must be accepted so long as it is not "'obviously wrong.'" *FTC v. Carter*, 636 F.2d 781,787-88 (D.C. Cir. 1980) (quoting *Texaco*, 555 F.2d at 877 n. 32).

Invention Submission Corp., 965 F.2d at 1089. This is the framework within which CVS's relevance claims must be assessed.

A copy of the resolution authorizing the use of compulsory process for this investigation was attached to the CID. Petition, Exhibit A at 3. In pertinent part it reads,

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

Id. The documents and information sought in the challenged CID specifications appear to fall well within the purpose of this investigation; that is, a determination of whether CVS's business operations might constitute "deceptive acts or unfair practices related to consumer privacy and/or data security in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act." Petition, Exhibit A at 3.

Indeed, CVS does not claim that the documents and information sought by Document Specifications 5, 6, or 7 and Interrogatories 1, 6, and 7 are unrelated to deceptive acts or unfair practices related to consumer privacy and/or data security.[6] It complains, rather, that these specifications seek documents and materials, relating to the electronically stored and retrievable personal information regarding its customers, that are unrelated to the events that triggered the Commission's interest in investigating CVS's data security practices in the first place: the dumpster incidents and ExtraCare Program data security vulnerability. Even in this regard, CVS's argument fails as to the data vulnerability with the ExtraCare Program because CVS's own description of this problem shows that it involved electronically stored and retrievable personal information about consumers. Petition at 9 ("Prior to June 20, 2005, the ExtraCare loyalty card program allowed ExtraCare members to obtain their recent purchase histories via a website request."). As previously noted, CVS has offered no legal support for its argument that the FTC may not conduct investigations about possible violations of law unless it already possesses some knowledge about each incident it wishes to investigate. Legal authority it does cite, the *Morton Salt* case in particular, flatly rejects CVS's argument. We find, therefore, both that the information sought by the challenged specifications is relevant to the purpose of this investigation, and that the investigation is in the public interest.

III. CVS Has Not Demonstrated that the FTC Lacks the Jurisdiction to Investigate CVS's Electronic Data Privacy and Security Acts and Practices.

[6] The challenged specifications deal with CVS's electronic security policies, practices and procedures, its policies, practices and procedures for evaluating the compliance and effectiveness of its electronic security policies, practices and procedures, and the identification of each instance in the last five years when unauthorized electronic access to a consumer's personal information has occurred. There is no legitimate basis for concluding that these specifications seek documents or information beyond the scope of the resolution authorizing the use of compulsory process in this investigation.

CVS claims that the FTC lacks jurisdiction to enforce privacy and data security standards related to protected health information ("PHI") within the meaning of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (Aug. 21, 1996) *as amended by* Pub. L. 105-33 (Aug. 5, 1997) *and* Pub. L. 105-34 (Aug. 5, 1997) ("HIPAA") because "Congress gave HHS exclusive administration and enforcement authority regarding data privacy and security issues under HIPAA." Petition at 20. CVS cites no authority for its claim that HHS has exclusive jurisdiction with respect to CVS's privacy and data security practices. Further, CVS cites no authority to support its claim that HIPAA somehow precludes the FTC from bringing an action against CVS for violations of Section 5 of the FTC Act relating to privacy and data security practices.[7]

Even if CVS's claim were correct, it would not provide sufficient grounds for quashing or limiting this investigatory CID. First, this is a coordinated investigation by HHS and the FTC. CVS cites no authority holding that the two agencies cannot conduct a coordinated investigation, eschewing redundant investigatory process service on CVS, which would be followed by post-investigation decisions regarding whether one agency or both agencies were better situated to deal with particular enforcement actions that might be uncovered during the course of these investigations. Second, "[a]n agency's investigations should not be bogged down by premature challenges to its regulatory jurisdiction." *Fed. Trade Comm'n v. Swanson*, 560 F.2d 1, 2 (1st Cir. 1977). "With rare exceptions (none of which applies here), a subpoena enforcement action is not the proper forum in which to litigate disagreements over an agency's authority to pursue an investigation." *Fed. Trade Comm'n v. Ken Roberts Co.*, 276 F.3d 583, 584 (D.C. Cir. 2001). Third, this is especially true where it

[7] CVS's Petition cites to public statements by current and former senior FTC officials to the effect that the Commission, as a matter of prosecutorial discretion, does not enforce HHS's privacy regulations under HIPAA. *See* Petition at 22 n. 38-39. Even so, the FTC has jurisdiction to remedy any violations of the FTC Act by CVS.

may not be possible to determine the scope of the jurisdictional claim until the investigation is substantially complete. *Fed. Trade Comm'n v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979) ("But where, as here, the FTC does not plainly lack jurisdiction, and the jurisdictional question turns on issues of fact, the agency is not obliged to prove its jurisdiction in a subpoena enforcement proceeding prior to the conclusion of the agency's adjudication."); *Fed. Trade Comm'n v. Monahan*, 832 F.2d 688, 689 (1st Cir. 1987) (Judge, now Justice, Breyer) ("We, like the FTC, must wait to see the results of the investigation before we know whether, or the extent to which, the activity falls within the scope of a[n] 'immunity'.").

IV. CVS Has Not Demonstrated that Caremark's Consumer Privacy and Data Security Practices Are Beyond the Scope of the Investigation.

CVS correctly notes that its Caremark subsidiary was acquired by it after the time of the events that gave rise to this investigation. Petition at 4 (Caremark "had no role in the incidents that form the basis of the inquiry, all of which occurred nearly two years before the 2007 merger."). CVS offers two reasons for excluding Caremark from the CID. Having already decided that CVS's electronic security is within the scope of the investigation, CVS's only remaining argument is that the CVS and Caremark "businesses are distinct." Petition at 18. CVS further argues that it "maintains a comprehensive firewall separating the businesses and records" of the parent and subsidiary firms. *Id*. That, however, does not provide a basis for eliminating Caremark from the CID. The Commission has reason to believe that the CVS and Caremark databases are interconnected. The information provided by CVS has not demonstrated that an intruder into the CVS system would be unable to gain access to sensitive personal information contained in the Caremark system. The Declarations of Nobles and Balnaves, Exhibits Y and Z respectively to the Petition, do not mention whether personal information is protected by the firewalls. The written firewall policy annexed to Exhibit Y applies to sensitive commercial information (such as prices and

contracts); it does not appear to address sensitive personal information at all. Accordingly, the Commission has no factual basis to conclude that continued investigation of CVS, including its Caremark subsidiary, is no longer in the public interest.[8]

V. CVS Has Provided No Factual Support for Its Claims that CID Compliance Would Be Burdensome.

Allegations of burden must be supported with specificity. *In re National Claims Service, Inc., Petition to Limit Civil Investigative Demand*, 125 F.T.C. 1325, 1328-29, 1998 FTC LEXIS 192, *8 (1998). *National Claims* teaches that, "[a]t a minimum, a petitioner alleging burden must (i) identify the particular requests that impose an undue burden; (ii) describe the records that would need to be searched to meet that burden; and (iii) provide evidence in the form of testimony or documents establishing the burden (e.g., the person-hours and cost of meeting the particular specifications at issue)." *Id*. CVS's Petition fails to meet this burden.

Even assuming that there were some merit in CVS's claims of burden, we have no factual basis upon which to rely in order to fashion a CID modification with respect to either its scope or the time within which compliance should occur. Additionally, any claim of burden must be assessed in the context of the size and scope of the investigation and of the Petitioner. CVS has provided no facts relative to these issues. Accordingly, the Commission has no reason to believe that CVS's compliance with the CID is likely to "pose a threat to the normal operation of [CVS's business] considering [its] size." *Fed. Trade Comm'n v. Rockefeller*, 591

[8] CVS's claim that the CID is defective, based on its speculation that procedures contained in the Commission's Operating Manual were not followed, Petition at 23-25, is without merit. The Operating Manual specifies internal operating procedures; it creates no rights enforceable by recipients of a CID, and CVS cites no authority to support its arguments based on the Operating Manual, even if it had a factual basis for its speculations.

F.2d 182, 190 (DC Cir. 1979).[9] Here, given the scope and scale of CVS's business, compliance with the CID seems unlikely to pose such a threat to CVS. The fact that compliance may be inconvenient or even of some burden is not a sufficient basis to quash or limit a CID. *Texaco*, 555 F.2d at 882 ("Some burden on subpoenaed parties is to be expected and is necessary in furtherance of the agency's legitimate inquiry and the public interest.").

VI. CONCLUSION AND ORDER

For all the foregoing reasons, **IT IS ORDERED** that CVS's Petition be, and it hereby is, **DENIED**. Pursuant to Rule 2.7(e), Petitioner must comply with the CID by August 18, 2008.

By direction of the Commission

[9] *See also Federal Trade Comm. v. Standard American, Inc*., 306 F.2d 231, 235 (3rd Cir. 1962) (finding petitioner had not provided sufficient evidence that compliance would lead to the "virtual destruction" of a business).