

ORIGINAL



**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

IN THE MATTER OF)
)
CVS CAREMARK CORPORATION)
)
_____)

0710122

**CVS CAREMARK CORPORATION'S
PETITION TO LIMIT OR QUASH CIVIL INVESTIGATION DEMAND**

Reed Smith, LLP
Anthony E. DiResta, Esq.
Mark S. Melodia, Esq.
Lawrence S. Sher, Esq.
Andrew R. Boortz, Esq.

1301 K. Street, N.W.
Washington, D.C. 20005
(202) 414-9200
(202) 414-9299 (fax)

Counsel for Petitioner

HIGHLY CONFIDENTIAL TREATMENT REQUESTED

! CONFIDENTIAL

TABLE OF CONTENTS

| | |
|---|----|
| INTRODUCTION AND SUMMARY..... | 2 |
| RELEVANT FACTS..... | 5 |
| The Dumpster Incidents | 7 |
| ExtraCare Program | 9 |
| The Challenged CID Specifications | 10 |
| LEGAL OBJECTIONS | 14 |
| 1. The Challenged Specifications Demand Documents and Information That Are Not Relevant to the Inquiry and Are Unreasonable | 14 |
| a. The Applicable Relevancy and Reasonableness Standard | 14 |
| b. The Challenged CID Specifications Seek Irrelevant Documents and Information and Are Unreasonable | 17 |
| 2. The Challenged Specifications Unreasonably Demand Documents and Information from Caremark and CVS Which Are Primarily Regulated by HHS and CMS as to Patient Privacy and Security Issues | 20 |
| 3. The CID is Defective and Should Be Quashed or Modified Because the FTC Failed to Follow its Own Rules and Operational Requirements Before Its Issuance..... | 23 |
| 4. Compliance with the Challenged CID Specifications Would Be Unduly Burdensome to CVS | 26 |
| CERTIFICATION..... | 30 |
| CONCLUSION | 28 |
| CERTIFICATE OF SERVICE..... | 30 |

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

IN THE MATTER OF
CVS CAREMARK CORPORATION

COMMISSIONERS:

William E. Kovacic, Chairman
Pamela Jones Harbour
Jon Leibowitz
J. Thomas Rosch

File No. P954807

CVS CAREMARK CORPORATION'S
PETITION TO QUASH OR LIMIT CIVIL INVESTIGATIVE DEMAND¹

Petitioner CVS Caremark Corporation ("CVS") petitions the Federal Trade Commission ("FTC"), pursuant to 16 C.F.R. §2.7(d), to quash or limit the Civil Investigative Demand ("CID") issued to CVS on May 20, 2008, pursuant to Section 20 of the FTC ACT, 15 U.S.C. § 57b-1.² By agreement of the FTC and counsel for CVS, the time to file this Petition was extended to June 20, 2008.³ Although CVS already has responded in part and produced responsive documents under the CID, counsel have been unable to agree upon the

¹ CVS requests that this Petition, as well as all supporting Exhibits, be maintained by the FTC as highly confidential. The information contained herein includes sensitive and proprietary business information of CVS. All such materials are intended only for review by the staffs of the FTC. Accordingly, CVS requests that this Petition and Exhibits receive the highest level of protection for confidentiality available under the Commission's Rules of Practice, *e.g.*, 16 C.F.R. § 4.10, the Freedom of Information Act, *e.g.*, 5 U.S.C. § 552(b)(3)(B); 15 U.S.C. § 57b-2(f), the Federal Trade Commission Act, *e.g.*, 15 U.S.C. §§ 46(f); 57b-2, and any other applicable statutes, regulations, and rules.

² See Exhibit A, May 20, 2008 CID issued to CVS.

³ See Exhibit B, June 6, 2008 Letter from Joel C. Winston, Associate Director, Division of Privacy and Identity Protection, FTC.

modifications to the CID requested by CVS, and accordingly, CVS respectfully petitions the FTC Commissioners to reasonably modify the CID as requested below.

INTRODUCTION AND SUMMARY

By this Petition, CVS seeks to quash or limit the CID issued by the FTC arising out of its inquiry related to: (1) CVS' physical disposal of CVS consumers' personal health information ("PHI") from its retail pharmacy stores and (2) the security of personal consumer information in CVS' ExtraCare program. In September 2007, the FTC initiated its non-public inquiry in conjunction with the Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) and served CVS with an extensive document and information request relating to its 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."⁴

CVS voluntarily cooperated with the FTC inquiry, provided information and voluminous documents relevant to the inquiry and corresponded with FTC Staff and Counsel repeatedly to address their questions and concerns. In April, 2008, counsel for CVS also met with FTC counsel and Staff and CVS voluntarily provided the Staff with a confidential memoranda responding to the inquiry, detailing the history of the dumpster incidents responsive to the inquiry, describing the efforts CVS has taken to protect PHI during trash disposal, and requesting that the inquiry be closed. The Staff declined to close its inquiry, and on May 20, 2008, the FTC issued the CID to CVS demanding production of documents and answers to interrogatories.

⁴ See Exhibit C September 27, 2007 Letter from FTC Staff to CVS.

On June 11, 2008, CVS submitted a written preliminary response to the CID, stating its legal objections to each challenged Specification and explaining the background of its ExtraCare loyalty card program and the efforts CVS had taken to protect personal information retained as part of its ExtraCare program. Nonetheless, the Staff still declined to close its inquiry and issued the CID even though CVS demonstrated that none of the dumpster or ExtraCare incidents resulted in the unauthorized access to sensitive customer accounts or information.

The CID seeks nine different Specifications for Documents and seven separate Specifications for Interrogatories from June 1, 2005, (and in some instances from June, 2003) to the present. CVS timely notified the FTC of its concerns and objections to the nature and scope of information requested in the CID and attempted, in good faith, to narrow and reasonably modify the Specifications sought in the CID. CVS agreed to provide and/or has already produced documents and information responsive to CID Specifications for Documents Numbers 1, 2, 3, 4, 8 and 9 and Specifications for Interrogatories Numbers 2, 3, 4, 5 and 8. This Petition relates only to CID Specifications for Documents 5, 6, 7 and Specifications for Interrogatories 1, 6, and 7, and the scope of "Company" in CID Definition No. 4.

The Specifications to which CVS has responded and produced documents relate to the inquiry into the protection of PHI arising out of the dumpster incidents or the protection of personal information in CVS' ExtraCare program described below. In contrast, the Specifications which CVS seeks to quash or limit by this Petition broadly demand a massive volume of documents and information regarding the security and confidentiality of CVS' electronically-stored, transmitted or electronically-accessible information that is not limited, or related at all, to: (1) the dumpster incidents or (2) the protection of the ExtraCare program

information. In compliance with the CID, CVS has produced copies of electronically-stored or transmitted documents (e-mails) relevant to the inquiry into both of these subjects.

CVS petitions the Commission to quash or modify the CID for the following reasons:

(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' 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' 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;⁵

(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 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.

Based on all of the facts and legal objections set forth below and in the Exhibits accompanying this Petition, CVS respectfully requests that the FTC quash or limit the CID to

⁵ In a good faith attempt to reasonably narrow the scope of the CID's definition of "Company," counsel for CVS and counsel for the FTC have had numerous recent exchanges concerning the nature of the systems and firewalls between the Caremark PBM business and CVS Pharmacy business. Such exchanges, however, have not resulted in a modification before the expiration of the deadline for filing this Petition.

seek production of documents and information that are relevant and reasonably related to the Staff's stated inquiry.

RELEVANT FACTS

CVS is the largest provider of prescriptions and related health care services in the nation. It has 190,000 employees in over 6,200 retail pharmacy locations in 40 states and the District of Columbia. On September 27, 2007 the Staff notified CVS in writing that it was conducting a "non-public inquiry into CVS Corporation's (CVS) practices for disposing of consumers' sensitive personal information."⁶ The FTC stated that its "inquiry stems from several television reports alleging that CVS improperly disposed of consumers' sensitive personal information ("dumping incidents")," based on accounts that consumer personal information was found in publically-accessible garbage dumpsters in and around Indianapolis, Indiana in June through September, 2006.⁷ Accordingly, the Staff advised CVS that through its inquiry it seeks "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."⁸

Thereafter, between September 2007 and May, 2008, as memorialized in several letters between counsel for CVS and the Staff, CVS provided information and documents relevant to the inquiry and worked diligently to cooperate and comply with the Staff's inquiry and requests for information.⁹ On April 7, 2008, CVS voluntarily provided the Staff with a confidential,

6 *See* Exhibit C.

7 *Id.*

8 *Id.*

9 The frequent and repeated correspondence between the FTC counsel and staff and CVS demonstrate CVS' efforts to cooperate and respond to the inquiry. *See* Exhibits D – N, Letters from CVS to FTC Staff dated November 13, 2007, February 1, 2008, March 17, 2008 (of which there were two), March 19, 2008,

comprehensive memorandum and documents responding to the inquiry, detailing the history of the dumpster incidents, describing the efforts CVS has taken to protect its disposal of PHI and reduce the likelihood of further dumpster incidents, and requesting that the inquiry be closed.¹⁰ Two days later, counsel for CVS met with FTC counsel and Staff to further discuss the inquiry and attempt to narrow the Staff's information requests. After the meeting, and even more voluntary production,¹¹ the Staff declined to close its inquiry. On May 20, 2008, the FTC issued the CID to CVS demanding production of documents and answers to interrogatories.

CID Specification No. 4, was the first time the Staff formally expressed its interest in information and documents relating to how CVS maintains personal information as part of its ExtraCare customer loyalty card Program. Thereafter, on June 11, 2008, CVS submitted its preliminary written response to the CID which identified the CID provisions CVS believed to be objectionable and explained the background of its ExtraCare customer loyalty card program and the efforts CVS had taken to protect any personal information retained as part of its ExtraCare program.¹²

Although counsel for CVS attempted to persuade the FTC to narrow or reasonably modify certain of the CID's Specifications, the Staff refused to agree to the modifications requested by CVS. On June 6, 2008, Associate Director Joel C. Winston granted CVS an extension of time to file a petition to quash or limit the CID.¹³ On June 11th and 20th, 2008,

March 26, 2008, April 3, 2008, April 14, 2008, and April 15, 2008; Letters from FTC Staff to CVS dated December 14, 2007, and March 4, 2008.

¹⁰ See Exhibit O, April 7, 2008 Confidential Memorandum from CVS to FTC Staff.

¹¹ See Exhibit P, May 1, 2008 Letter from CVS to FTC Staff.

¹² See Exhibits Q and R, Letters from CVS to FTC Staff dated June 3, 2008 and June 11, 2008.

¹³ See Exhibit S, June 16, 2008 Letter from FTC Staff to CVS.

CVS timely produced documents and information responsive to the CID, with the exception of the challenged broad Specifications and Definition which are the subject of this Petition.¹⁴

The Dumpster Incidents

Since January 1, 2005, CVS had in place a “Confidential Waste SOP,” or Standard Operating Procedures Manual that applied to all employees in its now more than 6300 retail pharmacies. As part of this program, CVS initiated an extensive Confidential Pharmacy Waste Management Program known as “the Blue Bag Program” which requires that all pharmacy waste, except food, be disposed of in blue bags and is kept securely in-store for pickup. The Blue Bag Program was designed to minimize the risk of improper disclosure of PHI. Waste with PHI, such as “pharmacy labels, receipts, vials, and bottles,” had to be sorted into distinct blue trash bags,¹⁵ while all other pharmacy waste (*e.g.*, food, bottles or papers with no patient information) would be placed in clear trash bags.

Since 2005, the Blue Bag Program has been part of CVS operations manuals, and is part of employees’ own job descriptions. CVS also continually has reminded store managers, pharmacy teams, and employees of the Blue Bag Policy, formally and informally. Sometimes these reminders are periodically scheduled. At other times, the reminders follow news reports of violations. CVS has voluntarily incurred millions of dollars in costs each year since its Blue Bag Program has been implemented nationwide.

On a few occasions, as CVS detailed in its April 7, 2008 Memorandum to the FTC, the media “discovered” and publicized unauthorized disclosures of customer information that were supposed to have been disposed of pursuant to CVS’ Blue Bag Policy. In July, 2006, WTHR-

¹⁴ See Exhibits Q and R; *see also* Exhibit T, Letter from CVS to FTC Staff, dated June 16, 2008, and Exhibit U, Letter from FTC Staff to CVS, dated June 19, 2008.

¹⁵ See Exhibit V, CVS-355 to CVS-361.

TV, an Indianapolis NBC affiliate, ran a report on disposal of pharmacy information claiming that customer PHI had been discovered in a dumpster.¹⁶ Subsequently, between September 2006 and May, 2007, other reporters in Indiana, Ohio, Kentucky, Arizona and Texas reported similar dumpster incidents involving CVS and others.¹⁷

Following the Indiana dumpster incidents, in August, 2006, the Office of the Indiana Attorney General advised CVS that a complaint had been filed by consumers against multiple CVS pharmacists in response to the Indiana reporter's July, 2006 broadcast.¹⁸ CVS responded to the Indiana Attorney General's Office, explained that CVS pharmacy personnel have been counseled to adhere strictly to CVS guidelines regarding the safeguarding of PHI, and that the Blue Bag Policy had been re-issued and was being re-enforced with store personnel, including audit compliance measures.¹⁹ Following this investigation, all cases against the CVS pharmacists were dismissed.

Following the dumpster incident in Texas, the Texas Attorney General issued a Civil Investigative Demand on CVS and ultimately brought an enforcement action against CVS for alleged state-law violations governing the disposal of personal information.²⁰ That suit has been settled through a Stipulated Settlement whereby CVS, *inter alia*, has agreed to implement a state-wide shredding program, pursuant to Texas state law requirements.

There is no indication that any of these dumpster incidents resulted in the unauthorized access to customer accounts. Clearly, none of these incidents in any way involved access to

16 See Exhibit W, CVS-3511 to -3518.

17 See Exhibit O.

18 *Id.* at p. 16, n. 74.

19 *Id.*

20 See Exhibit X, CVS-1254 to CVS-1255.

CVS' electronic storage or transmission of sensitive customer account information. In almost all instances, the reporters who picked through the dumpsters themselves were the only audience to these disclosures. Unless identified, contacted, and singled out by these reporters, no CVS customers have complained that their information has been improperly disclosed because of CVS's PHI disposal policies.

In compliance with the CID, CVS has produced documents and information relevant and responsive to the inquiry related to the dumpster incidents.²¹

ExtraCare Program

CID Specification for Documents No. 4 demands production of documents concerning CVS's turning off of a feature on its website that was previously available to registered users of its ExtraCare loyalty card program. This feature concerned data relating to consumer purchases made under flexible spending accounts (FSA) set up through the consumers' employers.

Prior to June 20, 2005, the ExtraCare loyalty card program allowed ExtraCare members to obtain their recent purchase histories via a website request. In order to receive a purchase history report, ExtraCare program members were required to submit to CVS information including: (1) their last name; (2) the zip code that was used to create the ExtraCare account; and (3) the sixteen (16) digit ExtraCare number (*e.g.*, telephone number, social security number, etc.). Once this required information was entered accurately into the web form, an e-mail with the related purchase history would be sent to the e-mail account linked to the customer's ExtraCare account.

As described in detail in CVS' June 11, 2008 Memorandum to the FTC, in June, 2005, ComputerWorld reported in a press release that it had "identified" a potential vulnerability in

²¹ CVS could not identify any patient-specific information because the Television stations involved refused to provide the information their reporters had "discovered" in the dumpsters.

the data security of the ExtraCare FSA program. The report apparently was initiated by a woman involved with a consumer interest group known as Consumers Against Supermarket Privacy Invasion and Numbering (“CASPIAN”). CASPIAN’s mission, as described on its website, is to fight supermarket “loyalty” or frequent shopper cards through a variety of tactics.²² Some of these tactics apparently include committing computer crime and identity theft to advance their particular mission.²³

As detailed in CVS’ June 11, 2008 Memorandum to the FTC, upon learning about CASPIAN’s press release, CVS immediately took action to enhance the ExtraCare program’s security features to prevent any unauthorized disclosures of personally-identifiable information. Upon investigation of the alleged “vulnerability” identified by CASPIAN, it was determined that the ExtraCare program resulted in no unauthorized breach of personally-identifiable information. The investigation further determined that the ExtraCare program could not have resulted in harm to consumers through unauthorized disclosures because the information contained in the program is not “personally identifiable information” as defined by the FTC.²⁴

In any event, in compliance with the CID, CVS produced documents that were relevant and responsive to Specification for Documents No. 4.

The Challenged CID Specifications

The CID Specifications which CVS seeks to quash or limit by this Petition broadly demand documents and information regarding the security and confidentiality of CVS’ electronically-stored, transmitted or electronically-accessible information that is not relevant, or related at all, to the inquiry concerning: (1) CVS’ practices in handling consumers’ personal

²² See <http://www.nocards.org/press/overview.shtml>.

²³ See Exhibit R.

²⁴ *Id.*

information in connection with the dumpster incidents and (2) the ExtraCare program. The challenged CID Specifications include the following:

SPECIFICATIONS FOR DOCUMENT PRODUCTION

5. Documents sufficient to set out in detail all policies, practices, and procedures relating to the security and confidentiality of personal information that: (a) CVS collects, processes, maintains, stores, transmits, or disposes of using computer equipment or networks or (b) is electronically accessible through CVS websites or otherwise (collectively, "electronic security policies"). Responsive documents should include, but may not be limited to, IS Security policies, procedures, and standards from the IS Security Administration (CVS - 4432).

6. Documents sufficient to set out in detail all policies, practices, and procedures relating to how CVS has evaluated compliance with and the effectiveness of its electronic security policies. Responsive documents should include, but not be limited to, overseeing or monitoring compliance with the electronic security policies and assessing risks to the security and confidentiality of personal information.

7. Documents sufficient to identify any instance in the last five (5) years of unauthorized electronic access to customers' personal information (referred to herein as an "incident") that: (a) CVS collected, processed, maintained, stored, transmitted, or disposed of using computer equipment or networks or (b) was electronically accessible through CVS websites or otherwise. Responsive documents should include, but not be limited to:

- (i) the date(s) over which each incident occurred;
- (ii) the location(s) of each such incident;
- (iii) how each such incident occurred, if known;
- (iv) what types of personal information were accessible or compromised in each such incident; and
- (v) what steps CVS took to address each such incident.

SPECIFICATIONS FOR INTERROGATORIES

1. Provide a full and complete description of each instance in the last five (5) years of unauthorized electronic access to customers' personal information

(referred to herein as an "incident") that: (a) CVS collected, processed, maintained, stored, transmitted, or disposed of using computer equipment or networks or (b) was electronically accessible through CVS websites or otherwise. This description should include, but not be limited to:

- (i) the date(s) over which each incident occurred;
- (ii) the location(s) of each such incident;
- (iii) how each such incident occurred, if known;
- (iv) what types of personal information were accessible or compromised in each such incident; and
- (v) what steps CVS took to address each such incident.

6. Provide a full and complete description of all policies, practices, and procedures relating to the security and confidentiality of personal information that: (a) CVS collects, processes, maintains, stores, transmits, or disposes of using computer equipment or networks or (b) is electronically accessible through CVS websites or otherwise (collectively, "electronic security policies").

7. Provide a full and complete description of all policies, practices, and procedures relating to how CVS has evaluated compliance with and the effectiveness of its electronic security policies, including, but not limited to, overseeing or monitoring compliance with the electronic security policies and assessing risks to the security and confidentiality of personal information.

May 20, 2008 CID at pp. 8, 10-12.

In addition, CVS petitions to quash or limit the overly broad definition in the CID that describes Company as follows:

4. The "**Company**" or "**CVS**" shall mean CVS Caremark Corporation, its wholly or partially owned subsidiaries, parents, holding companies, branches, franchises, unincorporated divisions, joint ventures, operations under assumed names, and affiliates and all directors, officers, employees, agents, consultants and other persons working for or on behalf of the foregoing.

May 20, 2008 CID at 1. Caremark, although today it is part of the CVS Caremark Corporation legal entity, is a PBM that does business separate and distinct from CVS' retail

pharmacy.²⁵ Caremark did not merge with CVS until March 2007, almost four years after the time period for which the CID demands production of Caremark documents. Although the CID broadly seeks documents and information concerning the storage, transmission and access of its electronic information with CVS' Caremark business segment, the Staff has never notified CVS of *any* alleged data privacy or security violations whatsoever involving Caremark.

In any event, CVS maintains a comprehensive firewall separating the businesses and records of CVS and Caremark.²⁶ As set forth in the declarations of CVS' Chief Compliance Officer and Chief Technology Officer, CVS' pharmacy business and Caremark's PBM business "maintain separate and distinct information systems and networks that are separated by firewalls managed independently by each organization."²⁷

As a PBM, Caremark is primarily regulated by the Office of Civil Rights (OCR) at the Department of Health and Human Services concerning compliance with the privacy rules applicable to its PHI under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").²⁸ In addition, Caremark is also regulated by the Administrator of the Center for Medicare and Medicaid Services ("CMS") which has primary administrative and enforcement authority with respect to the security rules applicable to Caremark's handling of PHI as a "covered entity" under HIPAA.²⁹

25 As is obvious from CVS' website, its retail pharmacy and Caremark PBM segments are distinct businesses. *See, e.g.*, <http://www.cvscaremark.com/our-company/our-businesses>

26 *See* Exhibit Y, Declaration of CVS Chief Compliance Officer Diane Nobles, dated June 18, 2008 (with attachment); Exhibit Z, Declaration of CVS Chief Technology Officer Peter Balnaves dated June 16, 2008.

27 *Id.*

28 Pub. L. 104-99 (1996). *See* 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000).

29 *See* 45 C.F.R. § 160.102; 65 Fed. Reg. 82,462, 82,568 (Dec. 28, 2000).

LEGAL OBJECTIONS

1. The Challenged Specifications Demand Documents and Information That Are Not Relevant to the Inquiry and Are Unreasonable

a. The Applicable Relevancy and Reasonableness Standard

By this Petition, CVS does not challenge the FTC's statutory authority to investigate practices which it determines may be deceptive or unfair trade practices when used in the course of trade under 15 USC § 45(a). It is well-established, however, that the FTC's subpoena powers are not limitless. While Congress has provided agencies with authority to conduct reasonable investigations through the use of investigatory tools such as administrative subpoenas and CIDs, the federal courts serve as a safeguard against agency abuse by retaining the power to enforce such subpoenas and CIDs. *See, e.g., SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1024 (D.C. Cir. 1978), *cert. denied*, 439 U.S. 1071 (1979) ("[T]he federal courts stand guard, of course, against abuses of their subpoena-enforcement processes . . .") (citing *United States v. Powell*, 379 U.S. 48, 58 (1964) and *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 208 (1946)). The reason Congress has refused to confer upon administrative agencies their own subpoena enforcement power is "to prevent potential agency abuse and ensure that targets of investigations are accorded due process." Sean Doherty, *Commodity Futures Trading Comm'n v. Collins: Is the Rationale Sound for Establishing an Exception to Subpoena Law for Tax Returns?*, 7 DePaul Bus. L.J. 365, 376 (1995).

The recognized standard in determining whether a CID should be quashed or limited in scope or breadth was adopted by the Supreme Court in *United States v. Morton Salt Co.*, 338 U.S. 632 (1950). There the Court enforced an FTC cease and desist order against a corporation which included a requirement that the corporation file certain reports with the FTC demonstrating its continued compliance with the cease and desist order. *Id.* at 634-636.

Although the Court enforced the decree in *Morton Salt Co.*, it recognized that “a governmental investigation into corporate matters may be of *such a sweeping nature and so unrelated to the matter properly under inquiry* as to exceed the investigatory power.” *Id.* at 652 (emphasis added)). Accordingly, the Court instructed that agency subpoenas or CIDs should not be enforced if it is determined that they demand information that is: (a) not “within the authority of the agency,” (b) “too indefinite,” or (c) not “reasonably relevant” to the inquiry.” *Id.*

Particularly relevant here, in enforcing the decree seeking production of documents in *Morton Salt Co.*, the Supreme Court emphasized that the defendant corporation did not make any “reasonable efforts” to “obtain reasonable conditions,” noting that the corporation had failed to raise “objection to the order’s sweep, nor asked any modification...” *Id.* 338 U.S. at 653. If the corporation had objected and presented evidence concerning the excessive scope or breadth of the decree, the Court observed, the corporation “could have obtained any reasonable modifications necessary.” *Id.* at 654. In contrast, here, CVS previously raised and provided its objections in writing and affirmatively sought reasonable modifications of certain of the Specifications from the FTC.

The agency subpoena enforcement standard enunciated in *Morton Salt Co.* has been consistently applied by the courts. As the court recognized in *SEC v. Arthur Young & Co.*, 584 F.2d at 1030 “[t]oday, then, “(t)he gist of the protection is in the requirement . . . that the disclosure sought shall not be unreasonable. Correspondingly, the need for moderation in the subpoena's call is a matter of reasonableness.” 584 F.2d at 1030. The court explained further that ““the requirement of reasonableness . . . comes down to specification of the documents to be produced adequate, but not excessive, for the purposes of the relevant inquiry.” 584 F.2d at 1030 (quoting *Oklahoma Press*, 327 U.S. at 209). The subpoena request must “not [be] so

overbroad as to reach into areas that are irrelevant or immaterial,” the court added, “the test is relevance to the specific purpose.” *Id.*, 584 F.2d at 1028, 1031.

Following *Morton Salt Co.*, the court in *SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d 512, 514 (10th Cir. 1980), confirmed that “[t]o obtain judicial enforcement of an administrative subpoena, an agency must show that the inquiry is not too indefinite, is reasonably relevant to an investigation which the agency has authority to conduct, and all administrative prerequisites have been met” (quoting *United States v. Powell*, 379 U.S. 48, 57-58 (1964)); accord *SEC v. Wall St. Transcript Corp.*, 422 F.2d 1371, 1375 (2d Cir.), *cert. denied*, 398 U.S. 958 (1970). Other courts following the *Morton Salt Co.* standard have recognized that the disclosure sought by an agency through compulsory process must be both relevant to the inquiry and reasonable. See *FTC v. Mt. Olympus Fin. LLC*, 211 F.3d 1278 (10th Cir. 2000) (“the documents requested were reasonably relevant to an inquiry clearly within the authority of the FTC”); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 471 (2d Cir. 1996) (“the disclosure sought must always be reasonable”); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1993)(CID enforced only “if the information sought is reasonably relevant”); *FTC v. Texaco, Inc.*, 555 F.2d 862, 881 (D.C. Cir. 1977) (“the disclosure sought shall not be unreasonable”).

The court in *FTC v. Mt. Olympus Fin. LLC*, 211 F.3d 1278, 2000 WL 419825 at *2, for example upheld an FTC CID where “the documents requested were reasonably relevant to” the FTC’s inquiry. The court emphasized that the requested documents were “clearly relevant to the investigation” and “could confirm or disprove specific allegations of wrongdoing” by the company being investigated. *Id.* The court also determined that the FTC CID in question was “not overly broad or unduly burdensome” because the FTC “narrowed the requested

documentation” to information directly relevant to the FTC inquiry.

b. The Challenged CID Specifications Seek Irrelevant Documents and Information and Are Unreasonable

CID Specifications for Documents Nos. 5, 6, and 7 and for Interrogatories Nos. 1, 6 and 7 are on their face overly broad, excessive, and unreasonable because they demand disclosure of massive amounts of CVS’ electronically-stored, transmitted or accessible information, dating back at least three to five years, that is not at all relevant to the inquiry concerning either (1) the dumpster incidents or (2) the ExtraCare loyalty card program, which are the only subjects of the inquiry in this case. Based on the CID’s definition of “Company,” these Specifications are further unreasonable because they demand documents and information, not only from CVS’ retail pharmacy operations, but also from its Caremark PBM segment, a separate business distinct from CVS’s retail pharmacy, that had no role in the incidents that form the basis of the inquiry which all pre-dated the 2007 merger.

The patent unreasonableness of the CID’s demands is illustrated by focusing on the fact that literal compliance would require CVS, for all of its 6000 pharmacy locations (and all of CVS’ affiliated entities, including, but not limited to Caremark), to produce documents and information relating to how CVS “collects, processes, maintains, stores, transmits, or disposes of using computer equipment or networks” or “is electronically accessible through CVS websites.” CID Specifications for Documents Nos. 5, 7; Interrogatories Nos. 1, 6. None of these documents and information are at all related to the physical disposal of consumer PHI arising out of the dumpster incidents, nor are they related to facts concerning the ExtraCare program. CVS already has produced thousands of documents and information to the FTC that are relevant to these incidents.

The unreasonableness of these CID Specifications is exacerbated further when the

CID's overly broad definition of "Company" is imposed. Aside from being part of the same legal entity as CVS, there is no factual basis to support the CID's demand for such documents and information from the separate and distinct Caremark PBM business. There is no allegation or suggestion that Caremark had any role whatsoever in the incidents that form the basis of the inquiry, as the CVS' merger with Caremark occurred years *after* the dumpster and ExtraCare program incidents. Nor has there even been an *any* alleged data privacy or security violations whatsoever regarding the Caremark PBM business. Nevertheless, the CID unreasonably demands documents and information concerning storage and security of electronic information from the Caremark business dating as far back as June 2003--four years *before* Caremark merged with CVS. Because their businesses are distinct and because CVS maintains a comprehensive firewall separating the businesses and records of the CVS retail pharmacy and Caremark PBM businesses, the documents and information sought by the CID are not relevant or related at all to the inquiry concerning protection of CVS' pharmacy customers' personal information arising from the dumpster incidents and ExtraCare program.

Where, as here, an agency's subpoena or CID demands documents or information deemed irrelevant, excessive or unreasonable, courts have held that the agency's demands should be modified. For example, in *United States Commodity Futures Trading Commission v. The McGraw-Hill Companies, Inc.*, 390 F. Supp. 2d 27 (D.D.C. 2005), the court held that the CFTC's subpoena for documents should be modified on the grounds that some of the agency's demands were "overly broad" and "unduly burdensome" in that "the request cover[ed] all data from any source" and "requir[ed] all documents that in any way reference the formulas" in question. *Id.* at 36. Particularly pertinent here, the court further modified the scope of the CFTC subpoena on the grounds that it broadly sought documents "without regard to [the]

McGraw-Hill entity” involved. *Id.* Accordingly, the court limited the subpoena to affect only one of McGraw-Hill’s divisions, rather than the entire McGraw-Hill entity, because the division in question was the only entity that was arguably involved in any allegations of violations. *Id.*

Other courts have modified or limited agency demands in a subpoena or CID based upon the overly-broad time period of the demands in relation to the inquiry. For example, in *In re Sealed Case (Administrative Subpoena)*, 42 F.3d 1412, 1420 (D.C. Cir. 1994), the court remanded to the district court to determine whether the information requested by the subpoena fell within the time period related to a “valid purpose” under the subpoena. Before ordering compliance with the subpoena, the court concluded that the relevance of the documents sought by the agency needed to be determined; *see also FTC v. Texaco, Inc.*, 555 F.2d 862, 881-882 (D.C. Cir. 1977) (“the district court is authorized to impose reasonable conditions and restrictions with respect to the production of the subpoenaed material if the demand is unduly burdensome”).

Unlike the CID at issue in *FTC v. Mt. Olympus Fin. LLC*, 211 F.3d 1278, the documents and information demanded by the challenged Specifications are not “clearly relevant to the investigation,” could not “confirm or disprove specific allegations of wrongdoing” by CVS, and have not been “narrowed” to seek information directly relevant to the FTC inquiry. As the court did in *United States Commodity Futures Trading Commission v. The McGraw-Hill Companies, Inc.*, the overly broad CID Specifications in this case should be reasonably modified to request only relevant documents and information. 390 F. Supp. 2d at 36. Further, as in *McGraw Hill Companies, Inc.*, the CID Specifications that, based on the CID’s overly-broad definition of “Company,” demand documents and information from Caremark “without

regard” to the entity involved in the agency’s inquiry, should be modified as well. *Id.*

The challenged CID Specifications demand documents “of such a sweeping nature and so unrelated to the matter properly under inquiry” such that they are not “reasonably relevant” and should not be enforced. *Morton Salt Co.* 338 U.S. at 652; *SEC v. Arthur Young & Co.*, 584 F.2d at 1030; *SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d at 514. The Supreme Court in *Morton Salt Co.* expressly contemplated that unreasonable agency subpoenas or CIDs should be modified or limited based upon a party’s reasonable objections to the FTC’s sweeping demands. 338 U.S. at 653-654. Unlike the corporation in *Morton Salt Co.*, CVS did timely raise its reasonable objections with the FTC and affirmatively sought reasonable modifications to the CID to limit its breadth, scope and burdensomeness. *Id.*

2. The Challenged Specifications Unreasonably Demand Documents and Information from Caremark and CVS Which Are Primarily Regulated by HHS and CMS as to Patient Privacy and Security Issues

The CID should also be quashed or modified because it demands documents and information from CVS and Caremark concerning personal privacy and security information about which HHS has exclusive administrative and enforcement authority. As a PBM, Caremark is already regulated by the OCR at HHS concerning compliance with the privacy rules applicable to its PHI under HIPAA.³⁰ In addition, Caremark is also regulated by the Administrator of CMS with respect to the security rules applicable to Caremark’s handling of PHI as a “covered entity” under HIPAA. Congress gave HHS exclusive administration and enforcement authority regarding data privacy and security issues under HIPAA.³¹ HHS delegated authority to CMS to administer and enforce the security rules under HIPAA.³²

30 45 C.F.R. §160.300 *et seq.*

31 *See* 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000).

32 *See* 68 Fed. Reg. 60,694 (Oct. 23, 2003).

Accordingly, it is unreasonable and unduly burdensome for CVS to comply with the FTC's broad investigative demands in the challenged Specifications because the FTC is not the primary regulator with respect to data privacy and security issues, and unlike HHS, the FTC does not have the Congressionally-delegated administrative or enforcement powers or responsibilities concerning these issues.

OCR has promulgated regulations and guidance under HIPAA for electronically-stored information concerning data privacy and security which CVS has consistently followed. *See* "Privacy of Individually Identifiable Health Information."³³ The relevant OCR standards require only "reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart" for the protection of electronically stored protected health information. These HHS rules require that a covered entity, such as CVS: (a) "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information;"³⁴ and (b) "reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart."³⁵ In contrast to HHS' elaborate and specific privacy and security regulations, the FTC has not issued *any* regulations pertaining to the disposal of PHI.³⁶

33 45 C.F.R. §164.500 *et seq.*

34 45 C.F.R. §164.530(c)(1).

35 45 C.F.R. §164.530(c)(2)(ii).

36 The incongruity of FTC action in the medical privacy context has been recognized previously. "[A]ny FTC action with regard to privacy for consumer health information would raise difficult issues of coordination, as the HIPAA privacy standards are already being implemented by the Department of Health and Human Services." *Privacy and the World Wide Web*, George B. Delta and Jeffrey H. Matsuura, Law of the Internet §6.03 (Aspen Publishers, Inc. 2008).

Because the FTC's inquiry began as a joint investigation with HHS, prior to the issuance of the CID, on September 18, 2007, CVS produced documents and information to the OCR at HHS demonstrating CVS' compliance with all applicable HIPAA regulations.³⁷ After receiving CVS' documents and information, the OCR has not requested any specific changes to CVS' (or Caremark's) policies or procedures for protecting PHI, nor has the OCR initiated any enforcement or other formal proceedings against CVS.

There is no dispute that the HHS-- not the FTC --is the primary federal regulator with exclusive administrative and enforcement authority over CVS (including Caremark's PBM) with respect to data privacy and security issues. Former FTC Chairman Majoras told Congress a few years ago that HIPAA and its Privacy Rule are not enforced by the Commission.³⁸ Associate Director Joel Winston did the same just over two years ago.³⁹ A regulated entity like CVS is entitled to one consistent set of data privacy and security regulations. It is therefore unreasonable and unduly burdensome for the FTC to demand that CVS comply with the CID Specifications demanding documents and information concerning the very data privacy and security issues over which HHS has exclusive Congressional authority to administer and enforce. Accordingly, the CID Specifications should be quashed or limited to exclude such information.

³⁷ See Exhibit AA, CVS-345 to CVS-346.

³⁸ Deborah Platt Majoras, Chairman of the Federal Trade Commission, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*, a prepared statement before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs (Mar. 10, 2005), available at <http://www.ftc.gov/os/testimony/050310idtheft.pdf>.

³⁹ Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, *Statement of Joel Winston*, a prepared statement before the U.S. House of Representatives, Subcommittee on Social Security of the House Committee on Ways and Means (Mar. 30, 2006) available at: <http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=4790>.

3. The CID is Defective and Should Be Quashed or Modified Because the FTC Failed to Follow its Own Rules and Operational Requirements Before Its Issuance

Pursuant to 16 C.F.R. §2.3, it is clear the FTC is only permitted to investigate matters in the “public interest.” The FTC cannot initiate an investigation or take other action “when the alleged violation of law is merely of private controversy and does not tend adversely to affect the public.” *Id.* The CID Specifications which broadly demand documents and information from CVS and Caremark regarding all electronically stored, transmitted and accessible information clearly do not relate to any alleged violations of law at all, much less any public controversy. Accordingly, the CID is defective and should not be enforced because this case is not a situation “[w]here the public interest requires” compulsory process. 16 C.F.R. §2.4.

In addition, pursuant to 16 C.F.R. § 2.6, the FTC is required to notify a party under investigation: (i) of the purpose and scope of the investigation and (ii) of the conduct constituting alleged violations that are under investigation. In its September 27, 2007 letter, the FTC stated the purpose of its inquiry as follows: “[W]e seek to determine whether CVS’s handling of sensitive information from or about consumers in connection with the preparation and sale of prescription medicines and supplies raises any issues under Section 5.” Other than the dumpster incidents and the ExtraCare program, the CID has failed to notify CVS of “the nature of the conduct constituting the alleged violation which is under investigation.” Certainly, with respect to Caremark, the FTC has failed to notify CVS of *any* alleged data privacy or security violations whatsoever.

The FTC’s own Operational rules specify that “[i]nvestigations may be authorized to inquire into . . . suspected violations of the law.” FTC Operating Manual 3.1.2.1 (2). This is in the nature of a requirement that the FTC has some probable cause or reasonable suspicion

predicate before commencing an investigation and issuing a CID. *See Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946) (discussing relationship between “probable cause” under a warrant and grand jury investigation and comparing with requirements that agency subpoenas be issued for “a lawfully authorized purpose” and upon a determination “that the documents sought are relevant to the inquiry,”...and are “not excessive, for the purposes of the relevant inquiry”). It is clear that an agency “cannot rely upon its broad investigatory powers to pursue ‘other wrongdoing, as yet unknown.’” *In re Sealed Case*, 42 F.3d at 1419 (concluding that OTS did not have “unfettered authority to cast about for potential wrongdoing” and “must articulate a valid statutory basis” in support of the purposes of its investigation).

In *FTC v. O'Connell Assocs., Inc.*, 828 F. Supp. 165, 170 (E.D.N.Y. 1993), the court recognized that a CID was required to “state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.” The court there upheld the FTC CID in question finding that the FTC had a “suspicion that the law [was] being violated.” *Id.* (quoting *Federal Trade Comm'n v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992), *cert. denied*, 431 U.S. 974 (1993)). In contrast, here, the CID arises only out of the dumpster and ExtraCare incidents. Accordingly the CID is not based on any suspicion that CVS violated any laws in connection with the electronic storage of customer PHI.

To CVS' knowledge, the Staff also failed to follow other requirements in its own Operating Manual before commencing its investigation in this case or issuing the CID. Before issuing a CID, the Staff must prepare a Memorandum in Support of the CID that “describ[es] with specificity the information needed, the reasons why the information is relevant in the

inquiry, and the cost and burden production will impose on target companies.” FTC Operating Manual 3.3.6.7.1. and 3.3.6.7.5.1. Further, had the FTC properly followed its own Operating Manual in this case, “[b]efore recommending the initiation of an investigation,” FTC “staff should [have] obtain[ed] information indicating the Commission is likely to have jurisdiction” and “that the practices to be investigated are not the primary responsibility of another federal or state or local agency. . . .” FTC Operating Manual 3.2.2.1.1. Further, a formal request by the Staff is required to obtain approval for a full investigation in the form of an internal memorandum. FTC Operating Manual 3.3.5.1.2. A Memorandum in support of a full investigation requires a discussion of several factors, including “the description of the practices at issue and their impact upon consumers,” and the “extent of consumer injury inflicted by the practices to be investigated.” FTC Operating Manual 3.3.5.1.4.

It is difficult to fathom how these requirements were fulfilled concerning the CID’s demands relating to electronic data security policies and information which have nothing whatsoever to do with the dumpster incidents or the ExtraCare program situation and which are the subject of primary regulation by other federal agencies. There has simply been no consumer injury (or allegation of injury) resulting from any breach of electronic data security policies of CVS’ pharmacy or Caremark businesses.

Accordingly, the CID is defective and should not be enforced because it is apparent that the Staff has not complied with its own rules and operating prerequisites before initiating its investigation and issuing the CID. *See SEC v. Blackfoot Bituminous, Inc.*, 622 F.2d at 514 (“[t]o obtain judicial enforcement of an administrative subpoena, an agency must show that . . . All administrative prerequisites have been met” (quoting *United States v. Powell*, 379 U.S. at 57-58); accord *SEC v. Wall St. Transcript Corp.*, 422 F.2d at 1375.

4. Compliance with the Challenged CID Specifications Would Be Unduly Burdensome to CVS

Apart from the fact that the CID broadly demands production of documents and information which are not relevant to the subjects of the inquiry, the Challenged Specifications are also unreasonable because they demand from CVS a sweeping, unprecedented volume of documents and information. For example, the CID demands documents and information from CVS (as broadly defined in CID Definition 8) concerning “all policies, practices and procedures” relating to how it “collects, processes, maintains, stores, transmits, or disposes of using computer equipment or networks” or that “is electronically accessible through CVS websites or otherwise.” CID Specifications for Documents 5-7. The CID seeks all documents and interrogatory answers dating back from June 1, 2005, and in some cases over five years ago, and demands that CVS produce all of these materials in less than 21 days from CVS’ receipt of the CID.

The CID is further unreasonable and unduly burdensome because it demands that CVS “redact personal information” as defined in the CID from all of its responses to the CID. CID Instruction No. 11. “Personal information” is expressly defined in the CID to include:

identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security Number; (f) a driver's license number; (g) a date of birth; (h) credit and/or debit card information, including credit and/or debit card number and expiration date; (i) health information, including prescription information, medication and dosage; prescribing physician; or insurance information; (j) employment history and other information contained in employment applications; (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (l) any information from or about an individual consumer that is combined with (a) through (k) above.

CID Definition No. 8.

The CID thus requires that before CVS produces all of the documents broadly demanded through the Specifications, CVS must: (i) determine what information is responsive; (ii) ascertain where the documents or information are physically located and/or electronically stored and who possesses knowledge responsive to each interrogatory; and then (iii) review and physically redact all such “Personal Information” from the responsive physical documents and electronic information. Furthermore, the CID demands that CVS accomplish all of these tasks as to all of the documents and information demanded in less than 21 days, in addition to CVS’ obligations simultaneously to respond to all of the other CID Specifications for Documents and Interrogatories which are not challenged in this Petition.

Considering the extraordinary breadth and scope of the Specifications demanded, the CID does not “provide a *reasonable period of time* within which the material so demanded may be assembled and made available for inspection and copying or reproduction,” as is required under 16 C.F.R. §2.7(b)(1)(emphasis added). Compliance with the challenged CID Specifications would result in an unreasonable and undue burden upon CVS in terms of time, cost and resources that would “unduly disrupt or seriously hinder normal operations of [its] business.” *United States Commodity Futures Trading Commission v. The McGraw-Hill Companies, Inc.*, 390 F. Supp. 2d at 35-36 (citing *FTC v. Texaco, Inc.*, 555 F.2d at 882) (corporation responding to agency subpoena should not have “to cull its files for data” that would “impose an undue burden” and finding subpoena requiring production of “all documents that in any way reference” the issue in question “would be unduly burdensome”).⁴⁰

⁴⁰ Courts that have more recently reviewed FRCP Rule 45 subpoenas seeking broad production of electronic information have likewise refused to enforce them where the subpoena imposed an undue or oppressive burden on the responding party. *See, e.g., Miller v. Holzmann*, 471 F. Supp. 2d 119, 122 (D.D.C. 2007)(refusing to order production pursuant to FRCP Rule 45 subpoena where requests were oppressive

The costs and employee time and resources CVS would need to expend to comply with the CID, and conduct the extensive review and redaction demanded, would be excessive. As the court did in *McGraw-Hill Companies, Inc.*, the CID in this case should be modified to limit the demands which are “excessively broad on their face and technically call for a larger volume of data than may have been intended” by the FTC so as to “not impose an impermissible burden” on CVS. *Id.*, 390 F. Supp. 2d at 35; *FTC v. Texaco, Inc.*, 555 F.2d at 881-882 (“the district court is authorized to impose reasonable conditions and restrictions with respect to the production of the subpoenaed material if the demand is unduly burdensome”). The Commission should similarly modify the excessive CID Specifications in this case to limit the impermissible burdens imposed upon CVS which threaten to seriously disrupt its normal business operations.

CONCLUSION

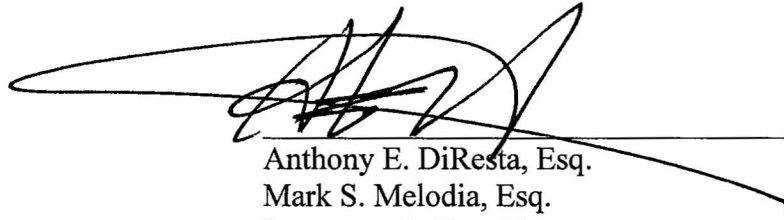
For all of the foregoing reasons, as well as those set forth in the accompanying Exhibits, CVS respectfully requests that the Commission quash or limit the challenged Specifications and provisions in the CID as set forth above.

and unduly burdensome as subpoena broadly sought production of all documents, including electronically stored versions without reasonable limitations); *Stevens v. National R.R. Passenger Corp.*, Civil Action No. 05-1924 (RCL), 2007 WL 1830869 at *4 (D.D.C. June 26, 2007) (granting motion to quash FRCP Rule 45 subpoena as unduly burdensome, where subpoena sought electronic records that were more than two years old).

Dated: June 20, 2008

Respectfully submitted,

REED SMITH, LLP

A large, stylized handwritten signature in black ink, appearing to be 'A. DiResta', is written over a horizontal line. The signature is highly cursive and extends significantly to the left and right of the line.

Anthony E. DiResta, Esq.

Mark S. Melodia, Esq.

Lawrence S. Sher, Esq.

Andrew R. Boortz, Esq.

1301 K. Street, N.W.

Washington, D.C. 20005


(202) 414-9200

(202) 414-9299 (fax)

Counsel for Petitioner

CERTIFICATION

Pursuant to 16 C.F.R. §2.7(d)(2), counsel for Petitioner CVS hereby certifies that they have conferred repeatedly with FTC counsel and staff by phone, email and letter correspondence in a good faith effort to resolve by agreement the modifications sought by this Petition, but have been unable to reach an agreement. CVS has agreed to respond to Specifications for Documents Nos. 1, 2, 3, 4, 8, and 9 and Specifications for Interrogatories Nos. 2, 3, 4, 5 and 8. These agreements are reflected in correspondence between CVS counsel and FTC counsel or FTC Associate Director Joel C. Winston, dated June 6 and June 19, 2008, which memorialize prior telephone conferences and correspondence between them.⁴¹

A handwritten signature in black ink, appearing to read 'Anthony E. DiResta', is written over a horizontal line. The signature is stylized and somewhat cursive.

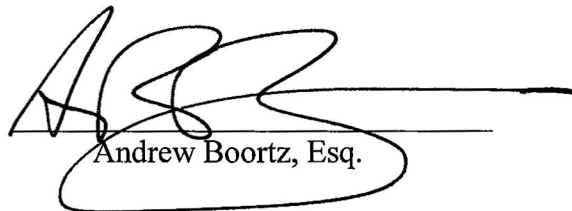
Anthony E. DiResta, Esq.

Counsel for Petitioner

⁴¹ See Exhibits B and U.

CERTIFICATE OF SERVICE

I hereby certify that on the 20th day of June, 2008, I caused the original and twelve (12) copies of Petition to Quash or Limit with attached Exhibits to be filed by hand delivery with the Secretary of The Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, D.C., 20580; and three (3) copies of same to be filed by hand delivery with Alain Sheer, Esq., Attorney, Division of Privacy and Identity Protection, Federal Trade Commission, 601 New Jersey Avenue, N.W., Washington, D.C., 20580



Andrew Boortz, Esq.