UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

[Redacted Public Record Version]

December 3, 2008

VIA FACSIMILE AND EXPRESS MAIL

CVS Caremark Corp.
c/o Anthony E. DiResta, Esquire
Reed Smith LLP
1301 K. Street, N.W.
Washington, DC 20005

Re: *Request for Rehearing of Denial of Petition to Quash or Limit Compulsory Process, In the Matter of CVS Caremark Corp.,* File No. 0723119

Dear Mr. DiResta:

This letter advises you of the Commission's disposition of CVS Caremark Corp.'s ("CVS") Request for Rehearing of Denial of Petition to Quash or Limit Compulsory Process ("Request for Rehearing") issued in conjunction with coordinated investigations of CVS's data security practices by the Federal Trade Commission (hereinafter "FTC" or "Commission") and the Office for Civil Rights of the Department of Health and Human Services ("HHS"). For the reasons stated below, the Letter Ruling by Commissioner Harbour, the Commission's delegate pursuant to 16 C.F.R. § 2.7(d)(4), Denying CVS's Petition to Limit or Quash CID (Aug. 6, 2008) ("Letter Ruling") is affirmed.[1]

I. Background and Summary.

Television reports from a number of cities around the United States indicated that some CVS stores were disposing of sensitive customer information by putting it in publicly-accessible trash containers. Some incidents were as recent as May 2007. In addition, in June 2005 media reports indicated that there were security vulnerabilities with CVS's computer storage of data relating to customer transactions covered by its ExtraCare loyalty card program.[2] The FTC

[1] CVS asked the Commission to stay or extend the return date established by the Letter Ruling, but failed to provide any substantial reason for the Commission to do so. Request for Rehearing at 1. The request for a stay is denied.

[2] CVS refers to these data security problems respectively as the "dumpster incidents" and the "ExtraCare program." Petition to Limit or Quash ("Petition") at 7, 9-10.

commenced an investigation, coordinated with a similar investigation by HHS under HIPAA,[3] to determine whether CVS's data security practices violate Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. On May 22, 2008, CVS received the CID that is the subject of this Request for Rehearing.

On June 20, 2008, CVS filed a timely Petition to Limit or Quash the CID. The Petition sought relief on the grounds that the CID sought information: (1) that was not relevant to the investigation; (2) that related to CVS's Caremark operation which was in no way implicated in the dumpster incidents or the ExtraCare program; (3) that includes protected health information that is exclusively regulated by HHS; (4) in a manner inconsistent with the FTC's internal rules and procedures; and (5) that would be unduly burdensome to produce. Letter Ruling at 2-3.

The Letter Ruling correctly observed that CVS has the burden to demonstrate that particular specifications of the CID were unreasonable, and that "the 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." Letter Ruling at 4 (citing *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) (internal citations omitted)). The Letter Ruling denied CVS's Petition because CVS had not provided adequate legal or factual support for its claims for relief from the CID.

On August 11, 2008, CVS filed its Request for Rehearing pursuant to 16 C.F.R. § 2.7(f). In its Request for Rehearing, CVS did not identify any specific legal or factual errors in the Letter Ruling but did attach a supplemental declaration providing some additional details regarding its burden arguments. Because CVS's appeal renewed all of the arguments presented in its original Petition, the Commission will review the Letter Ruling to determine whether it is factually and legally sustainable in light of the record, as supplemented.

CVS's primary claims are that its electronic security policies and procedures are outside the scope of the investigation[4] and that compliance with the specifications regarding electronic data security issues (Document Production Specifications 5-7, and Interrogatory Specifications 1, 6-7) is unduly burdensome.

---

[3] 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").

[4] Those arguments are addressed in Sections III and IV *infra*.

II. CVS's Burden Claims Regarding Its Electronic Security Policies Are Unsupported and Reflect a Mistaken View of the Scope of the CID.

First, CVS objects that Document Specification 7 and Interrogatory Specification 1[5] call for the company to produce massive amounts of information based on the possibility that review of those materials might turn up breaches of which CVS was not aware.[6] CVS's objection is predicated upon the misapprehension (which should have been corrected by raising it with staff as required by Commission Rule 2.7(d)(2)) that these specifications seek information about breaches that are unknown to CVS, rather than only those breaches – whether known to the public or not – of which CVS is aware. CVS claims to have already produced all of the information that it possesses regarding all "known instances of unauthorized electronic access to customers' personal information within the last five years."[7] If that is the case, it is unlikely that additional document production would be necessary to satisfy these specifications. CVS's arguments as to burden thus melt away.

CVS's estimation of the burden of complying with other specifications involving electronic data security is also overstated. Document Specifications 5-6 and Interrogatory Specifications 6-7 seek CVS's policies, practices, and procedures relating to electronic security and policies, practices, and procedures reflecting compliance and effectiveness of its electronic security procedures (including, for example, audit information). These types of documents and descriptions should not be voluminous by any means – if they were, the policies and procedures could not practicably be administered or enforced. They would primarily, if not entirely, be generated and maintained – and compliance with them monitored – in a central corporate office. Indeed, Mr. Pierce declares that he and others "oversee an IT security team . . . responsible for CVS' IT risk management, security and compliance activities." Pierce Decl. ¶ 3 at 2.

Thus, CVS has not met its burden to demonstrate factually that compliance with the CID would be unreasonable. In order to support quashing or limiting an investigatory CID, a movant must demonstrate with particularity, *In re National Claims Service, Inc., Petition to Limit CID*, 125 F.T.C. 1325, 1328-29, 1998 FTC LEXIS 192, *8 (1998), that the burden of complying with the CID is likely to "pose a threat to the normal operation of [CVS's business] considering [its]

---

[5] Document Specification 7 calls for documents "sufficient to identify any instance in the last five (5) years of unauthorized electronic access to customers' personal information . . . ." Interrogatory 1 seeks a "full and complete description" of any breaches corresponding to those in Document Specification 7.

[6] Pierce Decl. ¶ 26 at 10 ("I will next address the burdensomeness *if* Specification No. 7 and Interrogatory No. 1 were construed as requiring CVS to literally search for unknown instances of unauthorized electronic access to personal customer information for a five year period.").

[7] Pierce Decl. ¶ 9 at 5.

size," *Fed. Trade Comm'n v. Rockefeller*, 591 F.2d 182, 190 (D.C. Cir. 1979), such that it would be likely "to unduly disrupt or seriously hinder normal operations of" CVS's business. *Fed. Trade Comm'n v. Texaco, Inc.*, 555 F. 2d 862, 882 (3rd Cir. 1962). Based on the factual record of the Petition, even as supplemented, compliance with the CID poses no such threat to CVS. We agree with the Letter Ruling that CVS has not provided an adequate factual basis for its burden claims.

III. The CID Seeks Information that Is Relevant to the Investigation.

The Letter Ruling correctly determined that the scope of this investigation is determined by the resolution authorizing staff to utilize compulsory process, and that the specifications of the CID must be upheld so long as the information sought is "reasonably relevant" to that purpose and "not plainly incompetent or irrelevant to any lawful purpose" of the agency. Letter Ruling at 4-5; *Fed. Trade Comm'n v. Invention Submission Corp.*, 965 F.2d 1086, 1091-92 (D.C. Cir. 1992).

The resolution authorizing the use of compulsory process authorizes an investigation to determine whether any person has engaged in "deceptive acts or unfair practices related to consumer privacy and/or data security . . . in violation of Section 5 of the Federal Trade Commission Act." Request for Rehearing Exhibit B at 3. In asserting that information responsive to the CID is irrelevant, CVS's Petition attempts to narrowly define the investigation as related only to the dumpster incidents and the ExtraCare incidents, "the only subjects of the inquiry in this case." Petition at 17.[8] While those incidents were the initial impetus for the investigation, nothing in the CID resolution limits the scope of the investigation to the dumpster incidents and the ExtraCare program – the resolution authorizes the investigation of all of CVS's consumer privacy and data security practices. *See* Letter Ruling at 3-4.

CVS's counsel, in the Petition, asserts emphatically that CVS's data security practices are first rate despite the publicized incidents that sparked this investigation. *See, e.g.*, Petition at 13 ("CVS maintains a comprehensive firewall separating the businesses and records of CVS and Caremark"); *id.* at 21 ("OCR has promulgated regulations and guidance under HIPAA for electronically-stored information concerning data privacy and security which CVS has consistently followed"). *See also* Pierce Declaration, *e.g.* ¶ 20 ([*redacted*] [*redacted*] [*redacted*]). These statements may well be true, but the purpose of staff's investigation is to confirm the adequacy

[8] In support of its objection to the relevance of the CID specifications, CVS argues that the requests are unreasonably burdensome. *See, e.g.*, Petition at 17 ("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 . . . ."). As addressed in Section II, CVS's Petition vastly overestimates its compliance burdens.

of CVS's practices based upon a thorough independent review, not simply upon unsupported representations about those practices by counsel or declarants.

We agree with the Letter Ruling that, in light of the dumpster incidents (involving paper documents) and the ExtraCare vulnerability (involving data in electronic form), it is reasonable to examine CVS's data security and privacy practices comprehensively, not just the particular incidents that happen to have been publicized. Those incidents call into question the adequacy of CVS's data security policies and/or monitoring of compliance with policies for safeguarding personal information whether on paper or in electronic form. An inquiry limited to problems already identified would leave uninvestigated whether these incidents reflect fundamental problems with CVS's data security program. These are clearly questions that are "reasonably relevant" to the Commission's goal of enforcing Section 5 by ensuring companies take reasonable measures to protect consumers' personal information, and are "not plainly incompetent or irrelevant" to that lawful purpose. *Invention Submission Corp*., 965 F.2d at 1091-92.[9]

IV. The FTC Has Jurisdiction to Investigate CVS's Electronic Data Security Practices.

CVS cites no authority to support its claim that HHS has exclusive jurisdiction to enforce data privacy standards relating to information that can be considered protected health information under HIPAA, or, more importantly, that HHS's enforcement powers under HIPAA prevent the FTC from bringing an action against CVS for a violation of Section 5 of the FTC Act relating to its privacy and data security practices. Moreover, we agree with the Letter Ruling that it would be premature to resolve such a jurisdictional debate in the context of subpoena enforcement. *See, e.g., Fed. Trade Comm'n v. Roberts*, 276 F.3d 583, 584 (D.C. Cir. 2001) ("With rare exceptions . . . a subpoena enforcement action is not the proper forum in which to litigate disagreements over an agency's authority to pursue an investigation."). That is especially true where the jurisdictional issue turns on facts that need to be established during the course of the investigation. *Fed. Trade Comm'n v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979); *Fed. Trade Comm'n v. Monahan*, 832, F.2d 688, 689 (1st Cir. 1987).

We note that the data that was exposed in these breaches was not simply prescription data or other health-related information. As alleged in the Texas Attorney General's lawsuit against CVS arising from the disposal of information in a dumpster in Houston, for example, the customer information that was tossed out included credit card account numbers and driver's

[9] We reject the suggestion that the FTC's Operating Manual or *Oklahoma Press Publ'g Co. v. Walling,* 327 U.S. 186 (1946), require some showing akin to probable cause in order to demand information in a CID. Petition at 23-24. As noted in the Letter Ruling, the FTC's subpoena authority "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." *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950).

license numbers.[10] In that action, which was settled by CVS, the Texas Attorney General charged CVS with violating the Texas Identity Theft Enforcement and Protection Act, which applies to personal information such as credit card account numbers – but not to health-related information. While credit card and driver's license numbers can be considered protected health information under HIPAA when combined with health information, they clearly expose the customer to the risk of identity theft and are exactly the kinds of sensitive personal information that the Commission is charged with protecting under Section 5 of the FTC Act and other statutes (such as the Gramm-Leach-Bliley Act, the FACT Act of 2003, and the Fair Credit Reporting Act[11]) enforced by the FTC.

V. Caremark's Consumer Privacy and Data Security Practices Are Within the Scope of the Investigation.

CVS argues that the data security practices of its Caremark operation are beyond the scope of the investigation because it is not implicated in either the dumpster incidents or the ExtraCare program and because the Caremark side of the corporation was acquired only in March 2007. As noted above, the CID specifications are designed to determine whether the data security incidents that have come to light are aberrations or whether they reflect more pervasive problems with CVS's overall data security program, of which Caremark is now a part. The resolution permitting the use of compulsory process thus authorizes a complete and plenary review of CVS's data security practices, including those of its Caremark operation.

We recognize that the Extracare breach and many, but not all, of the dumpster incidents took place before the Caremark acquisition in March 2007, when it was under different management.[12] At the same time, Caremark's pre-acquisition data security measures likely inform its subsequent compliance; for example, certain Caremark pre-acquisition policies may have continued in force after the acquisition, and audits conducted prior to the acquisition may have revealed vulnerabilities in Caremark's data security program that were not addressed thereafter. Although CVS registered a general objection to providing information about the

[10] *See* www.oag.state.tx.us/newspubs/releases/2007/041607cvs_pop.pdf.

[11] Respectively codified as, 15 U.S.C. §§ 6801-09 and 6821-27, 15 U.S.C. §§ 1681-1681(x), and 15 U.S.C. §§ 1681-1681(u).

[12] CVS objects that 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." Petition at 18. Most of the specifications go back only to 2005, but one CID document specification and the corresponding interrogatory specification – seeking information about unauthorized electronic access to consumers' personal information – go back five years. According to the Pierce Declaration, at least, there are no known instances of unauthorized electronic access responsive to that document or interrogatory specification. Pierce Decl. ¶ 9 at 5.

Caremark operation on the basis that it was a separate business organization unconnected with the retail pharmacy operation,[13] aside from conclusory declarations[14] CVS did not adequately establish that fact in its correspondence with staff or in its Petition.

Moreover, as noted above, some of this material also bears on the post-acquisition privacy and security landscape at CVS. As indicated in Section II, the burden of producing material responsive to the Specifications – including materials relating to the Caremark entity – is likely to be modest as well. For all of these reasons, we affirm the Letter Ruling on this point.

VI. CVS's Allegations of Violations of the FTC Operating Manual Are Unfounded.

CVS's objection that the scope of the investigation extends beyond the dumpster incidents and the ExtraCare program is couched not only in terms of relevance, but also as a violation of the Commission's Operating Manual. Having concluded that a more comprehensive investigation is unreasonable and unwarranted, CVS speculates that the Commission's internal processes must have somehow gone awry. For the reasons stated above, we believe that a broader review of the company's data security program is reasonable, so we reject CVS's claim that process issued in this investigation in contravention of the general standards of conduct required of staff by the Operating Manual.[15]

---

[13] *See* Exhibits Q and R to Petition to Limit or Quash.

[14] *See* Exhibit Y (Nobles Declaration that she is "aware that a firewall policy exists between these businesses" and that the "firewall is maintained between the CVS pharmacy business and the Caremark PBM business to separate sensitive information that each business possesses"); Exhibit Y Attachment (CVS Caremark Firewall Policy). While the Nobles Declaration refers to "sensitive information," the attached firewall policy makes clear that it applies only to "competitively sensitive information," *e.g.* contracts, prices, and other financial arrangements, and does not on its face apply to personal information. *See also* Exhibit Z (Balnaves Declaration that the "CVS Pharmacy business and the Caremark PBM business unit maintain separate and distinct information systems and networks that are separated by firewalls managed independently by each organization" and that "both entities currently continue to operate under a separate set of security policies, procedures and standards"). This conclusion is not supported by any documentation or any detail about any firewalls or policies, procedures, or standards.

[15] We disagree that the CID Specifications or the CID issuance process violated the Operating Manual. In any case, the Operating Manual

> does not bind the Commission or its staff to procedures or policies that are not otherwise specifically mandated by the Procedures and Rules of Practice. Failure by the staff or the Commission to adhere to procedures outlined by this [Operating Manual] does not constitute a violation of the Rules of Practice nor

CVS also contends that there are no law violations at issue and that, because there is no specific allegation that the known breaches have led to consumer harm, Commission action is not in the public interest. We reject the argument that data breaches by one of the country's largest retail pharmacy chains are matters "merely of private controversy and do[] not tend adversely to affect the public." Petition at 23 (citing 16 C.F.R. § 2.3). Otherwise, the Commission would be powerless to investigate a series of data breaches, even if public accounts of the breaches indicated that the company was reckless in handling sensitive personal information that could be used for identity theft, unless the Commission could first demonstrate – without the benefit of any investigation – that the breaches had already been exploited. Investigating and remedying data security practices that may facilitate identity theft are clearly within the public interest and constitute a core mission of the FTC.[16]

VII. Order.

For the reasons set forth herein, the Letter Ruling should be, and it hereby is, **AFFIRMED**.

By direction of the Commission.

Donald S. Clark
Secretary

---

does it serve as a basis for nullifying any action of the Commission or the staff.

Operating Manual 1.1.1.; *see* Letter Ruling at 8 n.8.

[16] The Commission maintains a toll-free number (1-877-ID-THEFT) so consumers without Internet access can easily lodge ID theft complaints with the Commission, as well as a consumer education site available at www.ftc.gov/bcp/edu/microsites/idtheft/.