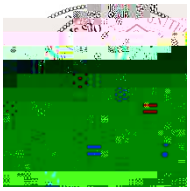

Office of the Secretary

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

[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 tao w

[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.*

[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

[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).

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

Respectively codified a

[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 and

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/.