United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

CVS Caremark Corporation
One CVS Drive
Woonsocket, Rhode Island 02895
Attn: Christine L. Egan, Esq., Assistant General Counsel

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

☐ You are required to appear and testify.

LOCATION OF HEARING	YOUR APPEARANCE WILL BE BEFORE
	DATE AND TIME OF HEARING OR DEPOSITION

☒ You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

☒ You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

June 11, 2008

3. SUBJECT OF INVESTIGATION

See attached Resolution.

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN	5. COMMISSION COUNSEL
Records Custodian: Joel Winston, Associate Director, Bureau of Consumer Protection Deputy Records Custodian: Loretta H. Garrison Senior Attorney, Bureau of Consumer Protection	Alain Sheer Federal Trade Commission, Bureau of Consumer Protection 600 Pennsylvania Avenue, NW, Stop NJ-3158 Washington, DC 20580

DATE ISSUED	COMMISSIONER'S SIGNATURE
5/20/08	

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature _____

Title _____

Sworn to before me this day

_____ _____

_____

Notary Public

_____

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY AND/OR DATA SECURITY

File No. P954807

Nature and Scope of Investigation:

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

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. 1.1 *et seq.* and supplements thereto.

By direction of the Commission.

Donald S. Clark
Secretary

Issued: January 3, 2008

CIVIL INVESTIGATIVE DEMAND
SCHEDULE FOR
PRODUCTION OF DOCUMENTS

To: CVS Caremark Corporation
One CVS Drive
Woonsocket, Rhode Island 02895
Attn: Christine L. Egan, Esq, Assistant General Counsel

I. DEFINITIONS

As used in this Civil Investigative Demand ("CID"), the words and phrases below have the following meanings:

1. "**And,**" as well as "**or,**" shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in the Schedule all information that otherwise might be construed to be outside the scope of the specification.

2. "**Any**" shall be construed to include "**all,**" and "**all**" shall be construed to include "**any.**"

3. "**CID**" means this Civil Investigative Demand, including the following Schedule and the attached "Resolution Directing Use of Compulsory Process in Non-Public Investigation of Unnamed Persons, Partnerships, Corporations and Others Engaged in Acts or Practices in Violation of Title V of the Gramm-Leach-Bliley Act and/or Section 5 of the FTC Act."

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.

5. "**Document**" shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, taped, recorded, filmed, punched, computer-stored, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book, electronic mail, and computer material (including print-outs, cards, magnetic or electronic tapes, discs and such codes or instructions as will transform such computer materials into easily understandable form).

6. "**Each**" shall be construed to include "**every**," and "**every**" shall be construed to include "**each**."

7. "**Identify**" or "**the identity of**" shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable.

8. "**Personal information**" shall mean individually 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.

9. "**Referring to**" or "**relating to**" shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

10. "**You**" and "**Your**" is the person or entity to whom this CID is issued and includes the "**Company**".

II. INSTRUCTIONS

1. **Applicable time period:** Unless otherwise specified, the relevant time period applicable to the specifications is from June 1, 2005, until the date of full and complete compliance with this CID. If CVS's forms, documents, policies, or procedures have changed during this period, please so state and briefly describe the nature of the change and its effective time period.

2. **Claims of Privilege:** If any document or information called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld stating individually as to each item:
   a. the type, specific subject matter, and date of the item;
   b. the names, addresses, positions, and organizations of all authors and recipients of the item; and
   c. the specific grounds for claiming that the item is privileged. If only some portion of any responsive document or information is privileged, all non-privileged portions of the document or information must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim or privilege. 16 C.F.R. § 2.8A(b).

3. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. *See* 15 U.S.C. § 50; *see also* 18 U.S.C. § 1505. If, for any specification, there are documents that would be responsive to this CID, but they were destroyed, mislaid, or transferred, describe the circumstances and date on which they were destroyed, mislaid, or transferred.

4. **Petitions to Limit or Quash:** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation.

5. **Modification of Specifications:** If you believe that the scope of either the required search, response, or any specification can be narrowed consistent with the Commission's need for documents, you are encouraged to discuss such possible modifications of this request, including any modifications of definitions and instructions, with Alain Sheer at 202-326-3321. All such modifications must be agreed to in writing by the Commission's

staff.

6. **Certification:** A responsible corporate officer or manager of the Company shall certify that the responses to the interrogatories and the documents produced or identified in response to this CID are complete and accurate and that the documents represent all documents responsive to this CID. This certification shall be made in the form set out on the back of the CID, or by a declaration under penalty of perjury as provided by U.S.C. § 1746.

7. **Scope of Search:** Documents covered by this CID are those in your possession or under your actual or constructive custody or control including, but not limited to, documents in the possession, custody, or control of your attorneys, accountants, directors, officers and employees, whether or not such documents were received from or disseminated to any person or entity.

8. **Document Production:** You shall produce the documentary material by making all responsive documents available for inspection and copying by the Commission's staff at your principal place of business. Alternatively, you may elect to send all responsive documents to Alain Sheer, Loretta H. Garrison, and Kristin Cohen, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Mail Stop NJ-3158, Washington, DC 20580. Because postal delivery in the Washington DC area and to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS. Notice of your intention to use this method of compliance shall be given by mail or telephone to Alain Sheer at 202-326-3321 at least five days prior to production.

9. **Document Identification:** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. In addition, number by page all documents in your submission and indicate the total number of documents in your submission.

10. **Production of Copies:** Unless otherwise stated, legible photocopies may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of original documents may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request.

11. **Redaction:** Unless expressly requested, redact personal information (*see* Definition 8)

from your responses.

12. **Submission of Electronic Data:** The following guidelines refer to any documents that you choose to provide in electronic form. You must confirm with the FTC that the proposed electronic data formats and media types will be acceptable to the government.

1. Magnetic and other electronic media types accepted
   a. CD-R CD-ROMs formatted to ISO 9660 specifications.
   b. DVD-ROM for Windows-compatible personal computers.
   c. IDE and EIDE hard disk drives up to 300GB per drive, formatted in Microsoft Windows-compatible, uncompressed data.

   Note: Other types of tape media used for archival, backup or other purposes such as 4mm & 8mm DAT and other cassette, mini-cartridge, cartridge, and DAT/helical scan tapes, DLT or other types of media **accepted only with prior approval.**

2. File and record formats
   a. E-mail: The FTC accepts MS Outlook PST files, MS Outlook MSG files. **Any other electronic submission of email accepted only with prior approval.**
   b. Scanned Documents: Image submissions accepted with the understanding that unreadable images will be resubmitted in original, hard copy format in a timely manner. Scanned documents must adhere to the following specifications:
   (1) All images must be multi-page, 300 DPI - Group IV TIFF files named for the beginning bates number.
   (2) If the full text of the document is available, that should be provided as well. The text should be provided in one file for the entire document or email, named the same as the first TIFF file of the document with a *.TXT extension.
   Note: Single-page, 300 DPI – Group IV TIFF files may be submitted **with prior approval** if accompanied by an acceptable load file such as a Summation or Concordance image load file which denotes the appropriate information to allow the loading of the images into a document management system with all document breaks (document delimitation) preserved. OCR accompanying single-page TIFF submissions should be located in the same folder and named the same as the corresponding TIFF page it was extracted from, with a *.TXT extension.
   c. Other PC files: The FTC accepts word processing documents in ASCII text, WordPerfect version 10 or earlier, or Microsoft Word 2002 version or earlier. Spreadsheets should be in MS Excel 2002 (*.xls) version or earlier. Database files should be in MS Access 2002 or earlier. PowerPoint presentations may be submitted in MS PowerPoint 2002 or earlier. **Other proprietary formats for PC files should not be submitted without prior approval.** Files may be submitted using the compressed ZIP format to reduce size and ease portability. Adobe Acrobat PDF (*.pdf) may be submitted where the normal business practice storage method is PDF.
   Note: Database files may also be submitted **with prior approval** as delimited ASCII text files, with field names as the first record, or as fixed-length flat files with appropriate record layout. For ASCII text files, field-level documentation

should also be provided and care taken so that delimiters and quote characters do not appear in the data. The FTC may require a sample of the data to be sent for testing.

3. Security

a. All submissions of electronic data to the FTC must be free of computer viruses. In addition, any passwords protecting documents or files must be removed or provided to the FTC.

b. Magnetic media shall be carefully packed to avoid damage and must be clearly marked on the outside of the shipping container: "MAGNETIC MEDIA – DO NOT X-RAY, MAY BE OPENED FOR POSTAL INSPECTION."

13. **Information Identification:** Each specification and subspecification of the CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification(s) or subspecification(s) to which it is responsive.

14. **Submission of documents in lieu of Interrogatory Answers:** Previously existing documents that contain the information requested in any written Interrogatory may be submitted as an answer to the Interrogatory. In lieu of identifying documents as requested in any Interrogatory, you may, at your option, submit true copies of the documents responsive to the Interrogatory.

III. SPECIFICATIONS FOR DOCUMENT PRODUCTION

Please provide:

1. All documents relating to corrective or disciplinary measures or actions CVS took to effect compliance with the CVS Blue Bag policy for each of the 187 stores identified in the February 2007 National In-Store Review (NIS) (CVS 2038) as not in compliance with the CVS Blue Bag policy.

2.

3. Documents sufficient to show how often each store received an . that included one or more questions or check-list items intended to evaluate the store's compliance with CVS policies relating to the security and confidentiality of personal information (including, but not limited to, its disposal). For each store, the information should: (a) report incidence for each calender year from 2005 through 2007 and by the job title of the reviewer (such as pharmacy supervisor; district manager; region manager; area vice president; and senior vice president), and (b) include a copy of the used by each reviewer, identified by the reviewer's job title, and identify the question(s) or check-list item(s) used to evaluate the store's compliance with CVS policies relating to the security and confidentiality of personal information.

4. On June 27, 2005, ComputerWorld reported that CVS "temporarily disabled a feature on its Web site after concerns were raised that unauthorized persons could improperly obtain customer-purchase records via e-mail. In a statement, Woonsocket, R.I.-based CVS acknowledged that it has turned off the feature that let registered users of its CVS ExtraCare loyalty cards request copies of their purchase data via e-mail and track purchases made under flexible spending accounts (FSA) set up through their employers. . . . CVS said it won't restore the FSA-tracking feature until it has developed 'additional security hurdles for accessing this purchase information.'" *See Privacy Fears Prompt CVS to Turn Off Online Service*, http://www.computerworld.com/securitytopics/security/story/0,10801,102773,00.html.

   Provide all documents relating to this alleged vulnerability, including: (a) how the alleged vulnerability occurred; (b) what types of personal information were contained in each account (*e.g.*, name, account number, purchase information, etc.) for the FSA-tracking feature; (c) what steps CVS took to address the alleged vulnerability, including the "additional security hurdles for accessing this purchase information" CVS employed for

these accounts; and (d) documents that evaluate, consider, respond to, acknowledge or contest the accuracy of or otherwise relate to the June 27, 2005, ComputerWorld news report.

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 such 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 acessible or compromised in each such incident; and

   (v) what steps CVS took to address each such incident.

8. All documents relating to the Liberty, Texas, dumping incident (referenced and defined in the FTC letter of September 27, 2007, n.1 and corresponding text) that:

   (a) assess, estimate, predict or count the number of consumers whose information was or may have been exposed in that incident and the amounts and types of information that was or may have been exposed;

   (b) evaluate, consider, respond to, acknowledge or contest the accuracy of or otherwise relate to the news reports of the Liberty, Texas, dumping incident;

(c) identify how, when, how many, and by whom consumers were notified that their information was or may have been exposed in that incident. If notification was made, explain why notification was made (*e.g.*, compelled by law) and provide a copy of each substantively different notification. If notification was not provided, explain why not; and

(d) identify the specific types of personal information found in the CVS dumpster in Liberty, Texas.

9. All documents relating to the monitoring of compliance with CVS's confidential waste disposal policies and procedures.

Responsive documents should include, but not be limited to, compliance audits conducted relating to CVS's disposal of personal information.

IV. SPECIFICATIONS FOR INTERROGATORIES:

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

2. Provide a full and complete description of how often each store received that included one or more questions or check-list items intended to evaluate the store's compliance with CVS policies relating to the security and confidentiality of personal information (including but not limited to its disposal) for each calender year from 2005 through 2007 and by the job title of the reviewer (such as pharmacy supervisor; district manager; region manager; area vice president; and senior vice president). In addition, identify the question(s) or check-list item(s) used to evaluate the store's compliance with CVS policies relating to the security and confidentiality of personal information.

3. State whether you agree that the

   did not provide reliable information about the extent to which pharmacy trash receptacles in CVS stores were being lined with blue confidential trash bags because the mystery shoppers conducting the survey: (1) could not observe all waste baskets in the pharmacies; (2) could not physically inspect pharmacy waste baskets because CVS did not authorize them to enter the pharmacies; and (3) conducted the survey by telephone. If you disagree with any of the three reasons set forth above, provide a full and complete explanation of the basis for your disagreement with each reason. If you believe that the provided accurate information about the extent to which pharmacy trash receptacles were being lined with blue confidential trash bags lines, provide a full and complete explanation of the basis for your belief.

4. State whether you agree that the did not require the mystery shoppers to observe, or report on, how blue bags taken from the

pharmacies were disposed of after being removed from pharmacy trash receptacles. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

5. State whether you agree that:

(a) the CVS Blue Bag policy in effect prior to July 2007 ("the policy") required pharmacy personnel in each store to sort trash to ensure that all confidential information was put into trash receptacles lined with blue trash bags and all non-confidential trash was put into receptacles lined with clear bags. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

(b) CVS did not recognize that pharmacy personnel would fail to sort confidential and non-confidential trash in the manner required by the policy. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

(c) after CVS learned about the WTHR television investigation, CVS concluded for the first time that CVS pharmacy personnel were not sorting trash in the manner required by the policy. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

(d) the CVS Blue Bag policy also required pharmacy or other store personnel in each store to place filled blue trash bags in a secure designated spot in the store's backroom for pickup by CVS warehouse trucks and to place filled clear trash bags in dumpsters or other garbage receptacles outside the store. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

(e) CVS did not recognize that pharmacy or other store personnel would fail to handle filled trash bags in the store's backroom in the manner required by the policy, resulting in blue trash bags, in some instances, being placed in unsecured publicly-accessible dumpsters. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

(f) after CVS learned about the WTHR television investigation, CVS concluded for the first time that CVS pharmacy or other store personnel were not handling filled trash bags in the store's backroom in the manner required by the policy. If you disagree with this statement, provide a full and complete explanation of the basis for your disagreement.

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.

8. If no documents are produced that are responsive for any of the entities identified in Document Specification 9, describe for each such group the basis for the statement