

thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true. Proposed respondent expressly denies the allegations set forth in the draft complaint, except for the jurisdictional facts, and expressly denies that the law has been violated.
6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent: (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the f

member, directly or indirectly.

3. Unless otherwise specified, “respondent” shall mean CVS Caremark Corporation, its subsidiaries, divisions, affiliates, and LLCs, and its successors and assigns.
4. “Personal information” shall mean individually identifiable information from or about an

complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with their compliance with Part II of this order, respondent, and its officers, agents, representatives, and employees, shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first year after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and

complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part II of this order; and

D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

owned, controlled, or operated by respondent or an LLC), current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within sixty (60) days after service of this order, and to such future subsidiaries and personnel within sixty (60) days after the respondent acquires the subsidiary or the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary (including an LLC), parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change of control.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

CVS CAREMARK CORPORATION

Dated: _____

By: _____

DIANE NOBLES

Senior Vice President and Chief Compliance Officer

JOEL WINSTON
Associate Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection

EILEEN HARRINGTON
(Acting) Director
Bureau of Consumer Protection