

)

072-3121

UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION

of r

COMMISSIONERS: Jon Leibowitz, Chairman  
William E. Kovacic  
J. Thomas Rosb  
Edith Ramirez  
Julie Brill

\_\_\_\_\_  
In the Matter of )  
)  
)

DOCKET NO. C-4308

1. Respondent Rite Aid Corporation is a Delaware corporation with its principal office or place of business at 30 Hunt Lane, Camp Hill, Pennsylvania 17011.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

## ORDER

### DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "store" shall mean each pharmacy entity or store location that sells prescription medicines, drug devices, supplies, or services and/or non-prescription products and services.
2. Unless otherwise specified, "LLC" shall mean a limited liability company: (a) that owns, controls, or operates one or more stores (including but not limited to, the companies identified in attached Exhibit A), and (b) in which Rite Aid Corporation is a member, directly or indirectly.
3. Unless otherwise specified, "Respondent" shall mean Rite Aid Corporation, its subsidiaries, divisions, affiliates, and LLCs, and its successors and assigns.
4. "Personal information" shall mean individually identifiable information from or about an individual consumer including but not limited to: (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 message identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license number or other government-issued identification number; (g) prescription information, such as medication and dosage, and prescribing physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) 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; (j) a biometric record; or (k) any information that is combined with any of (a) through (j) above. For the purpose of this provision, a "consumer" shall include an "employee," and an individual seeking to become an employee, where "employee" shall mean an agent, servant, salesperson, associate, independent contractor, and other person directly or indirectly under the control of Respondent.
5. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that Respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall not misrepresent in any manner expressly or by implication, the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumer

II.

IT IS FURTHER ORDERED that Respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumer. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards 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, 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 train 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 circumstance 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 I of this order, Respondent and its offices, 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.

IV.

IT IS FURTHER ORDERED that Respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, documents prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to, all plans, reports, studies, review audits, audit trails, policies, training materials, and assessments, and any other materials relating to Respondent's compliance with Parts I and II of this order, or the compliance pe

of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on November 12, 2030, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years;
- B. This order's application to any Re