

Complaint

IN THE MATTER OF

RITE AID CORPORATIONCONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATION OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket No. C-4308; File No. 072 3121**Complaint, November 12, 2010 — Decision, November 12, 2010*

The consent order addresses allegations that Rite Aid Corporation (“Rite Aid”) failed to protect the sensitive financial and medical information of its customers and employees, in violation of federal law. Specifically, the complaint alleged that Rite Aid failed to properly dispose of personal information, train employees, assess compliance with disposal policies and procedures, or establish procedures for discovering and resolving risks to personal information. The consent order requires Rite Aid to establish a comprehensive information security program to ensure the security, confidentiality, and integrity of personal information it collects from consumers and employees. The consent order further requires Rite Aid to have its security program independently audited by a third party every two years for the next 20 years to ensure compliance.

Participants

For the *Commission*: *Kristin Krause Cohen, Loretta H. Garrison, and Alain Sheer.*

For the *Respondent*: *Stephen Paul Mahinka, Morgan Lewis & Bockius.*

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that Rite Aid Corporation (“Respondent” or “Rite Aid”) has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Rite Aid is a Delaware corporation with its principal office or place of business at 30 Hunter Lane, Camp Hill, PA 17011. It conducts business through several wholly-owned subsidiaries and limited liability companies.

Complaint

2. The acts and practices of Respondent as alleged in this complaint are in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT’S BUSINESS

3. At all relevant times, Respondent has been in the business of selling prescription and non-prescription medicines and supplies, as well as other products. It operates, among other things, approximately 4,900 retail pharmacy stores in the United States (collectively, “Rite Aid pharmacies”) and an online pharmacy business. Respondent allows consumers to pay for their purchases with credit, debit and electronic benefit transfer cards (collectively, “payment cards”); insurance cards; personal checks; or cash.

4. In conducting its business, Respondent routinely obtains information from or about its customers, including, but not limited to, name; telephone number; address; date of birth; bank account number; payment card account number and expiration date; prescription information, such as medication and dosage, prescribing physician name, address, and telephone number, health insurer name, and insurance account number and policy number; and Social Security number (collectively, “personal information”). Respondent also collects personal information from or about employees and job applicants, including, but not limited to, Social Security number.

5. Respondent operates computer networks in its pharmacies, corporate headquarters, and distribution centers. Among other things, Respondent uses the networks to fill orders for prescription medicines and supplies; process sales, including to obtain authorization for payment card and insurance card transactions; and aggregate, store, and transmit personal information.

Complaint

RESPONDENT'S REPRESENTATIONS

6. Respondent has disseminated or caused to be disseminated statements and privacy policies to consumers regarding the privacy and confidentiality of personal information, including, but not limited to:

- a. From at least 2003, the following statement in its Notice of Privacy Practices:

Rite Aid takes its responsibility for maintaining your protected health information in confidence very seriously. Protected health information means information about you that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services. It also includes basic demographic information. We are required by law to maintain the privacy of protected health information and to provide you with a Notice of Privacy Practices including our legal duties with respect to protected health information. (See Exhibit A).

- b. From at least 2004, the following statement in a brochure seeking its customers' medical history:

Although you have the right not to disclose your medical history, Rite Aid would like to assure you that we respect and protect your privacy. (See Exhibit B.)

RESPONDENT'S SECURITY PRACTICES

7. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information. Among other things, Respondent has failed to: (1) implement policies and procedures to dispose securely of such information, including, but not limited to, policies and procedures to render the information unreadable in the course of disposal; (2) adequately train employees to dispose securely of such information; (3) use reasonable measures to assess compliance with its established policies and procedures

Complaint

for the disposal of such information; and (4) employ a reasonable process for discovering and remedying risks to such information.

8. As a result of the failures set forth in Paragraph 7, Respondent discarded materials containing personal information in clear readable text (such as pharmacy labels and employment applications) in unsecured, publicly-accessible trash dumpsters used by Rite Aid pharmacies on numerous occasions. For example, in late 2006 and continuing into 2007 and 2008, television stations and other media outlets reported finding personal information in unsecured dumpsters used by Rite Aid pharmacies in at least 7 cities throughout the United States. The personal information found in the dumpsters included information about Respondent's customers and job applicants. Information discarded in publicly-accessible dumpsters could be misused to commit identity theft or to steal prescription medicines.

VIOLATIONS OF THE FTC ACT

9. Through the means described in Paragraph 6, Respondent represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect personal information against unauthorized access.

10. In truth and in fact, Respondent did not implement reasonable and appropriate measures to protect personal information against unauthorized access. Therefore, the representation set forth in Paragraph 9 was, and is, false or misleading.

11. As set forth in Paragraph 7, Respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information. Respondent's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

12. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices, in or

Complaint

affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this twelfth day of November, 2010 has issued this complaint against Respondent.

By the Commission.

Complaint

EXHIBIT A

The Health Insurance Portability and Accountability Act ("HIPAA")

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION
ABOUT PATIENTS MAY BE USED AND DISCLOSED
AND HOW PATIENTS CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

Rite Aid will ask you to sign an Acknowledgment that you have received this Notice of Privacy Practices ("Notice"). This Notice describes, in accordance with the HIPAA Privacy Regulation, how Rite Aid may use and disclose your protected health information to carry out treatment, payment or health care operations and for other specific purposes that are permitted or required by law. The Notice also describes your rights and Rite Aid's duties with respect to protected health information about you.

Rite Aid will store information provided by you in the computer system. That information will include your name, address, phone number and other identifying information. In addition, any information that you provide concerning drugs that you are taking, medical conditions you may have, allergies, and other matters affecting your health will be stored in the computer.

TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

We will use your health care information to treat you. For example, we will use health care information to dispense prescription medications. We may also disclose your information to other health care providers for the purpose of treatment.

We will use your health care information to receive payment for products and services. For example, we may contact your third party payor (for example, insurer or pharmaceutical benefits manager) to determine whether your program will pay for your prescription. We will bill you and/or a third party payor for the cost of prescription medications dispensed to you. The information on or accompanying the bill may include your identification, as well as the prescriptions you are taking.

We will use your health care information to carry out health care operations. For example, we may use information in your health record to monitor the quality of pharmacist performance and to train pharmacy personnel.

USES AND DISCLOSURES THAT ARE EITHER PERMITTED OR REQUIRED BY THE REGULATION

Using their judgement as health care professionals, our pharmacists may disclose your protected health information to a family member, other relation, close personal friend, or any person you identify as being involved in your health care.

We form contracts with some entities known as Business Associates to perform services for us. For example, we sometimes require Business Associates to sort insurance or other third party payor claims for submission to the actual payor. We may disclose protected health information to our Business Associates so that they can perform the job we asked them to do, then bill your third party payor for services rendered. We require the Business Associates to appropriately safeguard the protected health information.

Complaint

EXHIBIT A

We may contact you to provide refill reminders or information about treatment alternatives or other health related benefits and services that may be of interest.

OTHER REQUIRED OR PERMITTED DISCLOSURES

We may disclose your health care information to the following entities and/or under given circumstances:

- to the Food and Drug Administration (FDA) relative to adverse events regarding drugs, foods, supplements, and other health products or to post marketing surveillance to enable product recalls, repairs, or replacement;
- to public health or legal authorities charged with preventing or controlling disease, injury, or disability;
- to law enforcement agencies as required by law or in response to a valid subpoena or other legal process;
- to health oversight agencies (medical licensing boards, e.g.) for activities authorized by law such as audits, investigations, and inspections necessary for Rite Aid's licensure and for the government to monitor the health care system, etc.;
- in response to a court order, administrative order, subpoena, discovery request, or other lawful process by another person involved in a dispute involving a patient, but only if efforts have been made to tell the patient about the request or to obtain an order protecting the requested health care information;
- as authorized by and as necessary to comply with laws relating to worker's compensation or similar programs established by law;
- whenever required to do so by law;
- to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of the patient's information;
- to a coroner or medical examiner when necessary, for example, to identify a deceased person or to determine a cause of death, or to funeral directors consistent with applicable law to carry out their duties;
- to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant, consistent with applicable law;
- to contact the patient for the purpose of fundraising;
- to notify, or assist in notifying, a family member, personal representative, or another person responsible for the patient's care, of the patient's location, or general condition;
- to a correctional institution or its agents, if a patient is or becomes an inmate of such an institution, when necessary for the patient's health or the health and safety of others;
- when necessary to prevent a serious threat to the patient's health and safety or the health and safety of the public or another person;
- as required by military command authorities, when the patient is a member of the armed forces, and to appropriate military authority about foreign military personnel;
- to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law;
- to authorized federal officials so they may provide protection to the president, other authorized persons, or foreign heads of state or conduct special investigations;
- to a government authority, such as a social service or protective services agency, if Rite Aid reasonably believes the patient to be a victim of abuse, neglect, or domestic violence, but only to the extent required by law, if the patient agrees to the disclosure, or if the disclosure is allowed by law and Rite Aid believes it is necessary to prevent serious harm to the patient or to someone else or the law enforcement or public official that is to receive the report represents that it is necessary and will not be used against the patient.

MORE STRINGENT LAWS

If your state has a law or regulation that is more stringent than the HIPAA Regulation, please refer to the accompanying page where that more stringent law will be reflected.

Complaint

EXHIBIT A**AUTHORIZED USE AND DISCLOSURE**

We will obtain your written Authorization before using or disclosing protected health information about you for purposes other than those listed above or otherwise permitted or required by law. You may revoke an Authorization in writing at any time. Such revocations must be made in writing. Forms for making revocations, which are available in Rite Aid pharmacies, should be completed and sent to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. Upon receipt of the written revocation, we will stop using or disclosing protected health information about you, except to the extent that we have already taken action in reliance on the Authorization.

THE PATIENT'S RIGHTS**RESTRICTION REQUESTS**

You have the right to request that we restrict how your protected health information is used or disclosed in carrying out treatment, payment, or health care operations. Such requests must be made in writing to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. We are not required to agree to the requested restrictions. If however, we do agree to the requested restrictions, that agreement will be binding on us.

ALTERNATIVE MEANS OF COMMUNICATION

You have the right to request that our communications to you concerning your health care information be made by alternative means or at alternative locations. For example, you may wish us to communicate in some way other than mailing to your home address or calling your home telephone number. Such requests must be made in writing to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. We will comply with a reasonable request for such an alternative.

ACCESS

You have the right to inspect and obtain a copy of your protected health information. You have the right to access and copy protected information about you contained in the designated record set for as long as we maintain your protected health information. The designated record set usually will include prescription and billing records. To receive a copy of your protected health information, you must send a written request to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. Forms for making Access requests are available in our pharmacies. We may charge you a fee for the costs of copying, mailing, or other supplies that are necessary to grant your request. We may also deny your request to inspect and copy in limited circumstances. If you are denied access to your protected health information in most cases you may request that the denial be reviewed.

HEALTH CARE INFORMATION AMENDMENTS

If you feel that the protected health information we maintain about you is incomplete or incorrect, you may request that we amend it. You may request an Amendment for as long as we maintain the protected health information. A request for an Amendment must be made in writing. Forms for making such requests, which are available in our pharmacies, should be completed and sent to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. You must include a reason that supports your request. In certain cases, we may deny the request. If the request for Amendment is denied, you have the right to file a statement of disagreement with the decision, and we may give a rebuttal to your statement.

ACCOUNTING

FEDERAL TRADE COMMISSION DECISIONS
VOLUME 150

Complaint

EXHIBIT A

For most purposes other than treatment, payment, or health care operations, you have the right to receive an Accounting of the disclosures we made, on or after April 14, 2003, of your protected health information. The Accounting will exclude disclosures we may have made directly to you, disclosures to friends or family members involved in your care, and disclosures for purposes you specifically authorized in writing. The right to receive an Accounting is subject to certain other exceptions, restrictions, and limitations. A request for an Accounting must be made in writing. Forms for making such requests, which are available in our pharmacies, should be completed and sent to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. The time period for the requested accounting must be specified and it may not be longer than six years. The first Accounting you request within a 12-month period will be provided free of charge, but you may be charged for the cost of providing additional Accountings within that period. We will notify you of the cost involved and you may choose to withdraw or modify the request at that time.

NOTICE OF PRIVACY PRACTICES

You have a right to receive a paper copy of this Notice from us upon request even if you have already received the Notice electronically (for example, on the Internet).

RITE AID'S DUTIES

Rite Aid takes its responsibility for maintaining your protected health information in confidence very seriously. Protected health information means information about you that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services. It also includes basic demographic information. We are required by law to maintain the privacy of protected health information and to provide you with a Notice of Privacy Practices including our legal duties with respect to protected health information. In addition, Rite Aid is required to abide by the terms of the Notice that is currently in effect.

We reserve the right to change the terms of our Notice and to make the new Notice provisions effective for all protected health information that we maintain. When we makes changes in our Notice, copies of the revised Notice will be available on request in all our pharmacies. A copy will be posted in all of our pharmacies and will be available on our web site at www.riteaid.com.

FOR MORE INFORMATION OR TO REPORT A PROBLEM

If you have questions or would like additional information about our privacy practices, you may contact the Privacy Office at (717) 761-2633 or by writing to the Privacy Office, Rite Aid, P.O. Box 3165, Harrisburg, PA 17105. Forms for filing a written complaint to Rite Aid are available at our pharmacies. If you believe your privacy rights have been violated, you can file a complaint with Rite Aid's Privacy Office or with the Secretary of Health and Human Services. There will be no retaliation for filing a complaint.

EFFECTIVE DATE

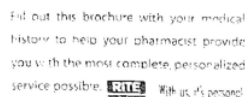
This Notice of Privacy Practices is effective as of April 14, 2003.

EXHIBIT B

RAC001574

Your PC: AID Pharmacist

With us, it's personal.



CONFIDENTIAL

Medical Information

Please check the appropriate box(es)

[illegible]

Last	First	Middle Initial
-------------	--------------	-----------------------

Street or P.O. Box Apt. #

City _____ State _____ Zip _____

Telephone

E-mail Address

Date of Birth (Month/Day/Year)

Gender (circle one): **MALE** **FEMALE**

If you have children in your household, to prevent accidental drug poisoning, please specify child resistant packaging.

Would you like us to dispense your medications in child resistant packaging?

☐ YES ☐ NO

Prescription Insurance

☐ YES ☐ NO

☐ YES ☐ NO
If yes, name cardholder

Cardholder's Name

RAC Relationship to cardholder (circle one)
 1 Cardholder, spouse, child, dependent parent,
 disabled descendant, full time student, other

KNOWN ALLERGIES AND DRUG REACTIONS

- ☐ No known allergies/drug reactions
- ☐ Aspirin
- ☐ Cephalosporins (ex. Cefclor, Keflex)
- ☐ Codeine
- ☐ Erythromycin
- ☐ Penicillins
- ☐ Sulfa drugs
- ☐ Tetracyclines
- ☐ Xanthines (ex. Theophylline)

HEALTH CONDITIONS

- ☐ Angina
- ☐ Anemia
- ☐ Arthritis
- ☐ Asthma
- ☐ Blood clotting disorders
- ☐ Blood pressure, high
- ☐ Breast feeding
- ☐ Cancer
- ☐ Diabetes
- ☐ Heart conditions
- ☐ Kidney disease
- ☐ Liver disease
- ☐ Lung disease
- ☐ Parkinson's disease
- ☐ Pregnancy
- ☐ Ulcers

Other allergies and drug reactions

Other health conditions

List of prescriptions you are currently taking
which were NOT purchased in this store _____

List of non-prescription medications you are currently taking _____

PHARMACISTS COMMENTS

This information is requested by your Fire Aid Pharmacist as required by state regulation so that he or she can provide appropriate pharmacy services to you. This information will be kept confidential. Since health information may change periodically please notify your Fire Aid Pharmacist of any changes in medications (prescription and non-prescription), allergies, drug reactions or health conditions.

Signature _____

Date _____

Signature _____

DO NOT WISH TO COMPLETE THIS FORM

Date _____

RAC001575

Decision and Order

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

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

Decision and Order

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, drugs, 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) 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; (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

Decision and Order

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 consumers.

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 consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain

Decision and Order

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 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

Decision and Order

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

Decision and Order

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, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment.

Decision and Order

V.

IT IS FURTHER ORDERED that Respondent Rite Aid Corporation shall deliver a copy of this order to all its current and future subsidiaries (including LLCs and each store that is 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 in Respondent's name or address. *Provided, however,* that, with respect to any proposed change in Respondent about which Respondent learns less than thirty (30) days prior to the date such action is to take place, Respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division 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

Decision and Order

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 Respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

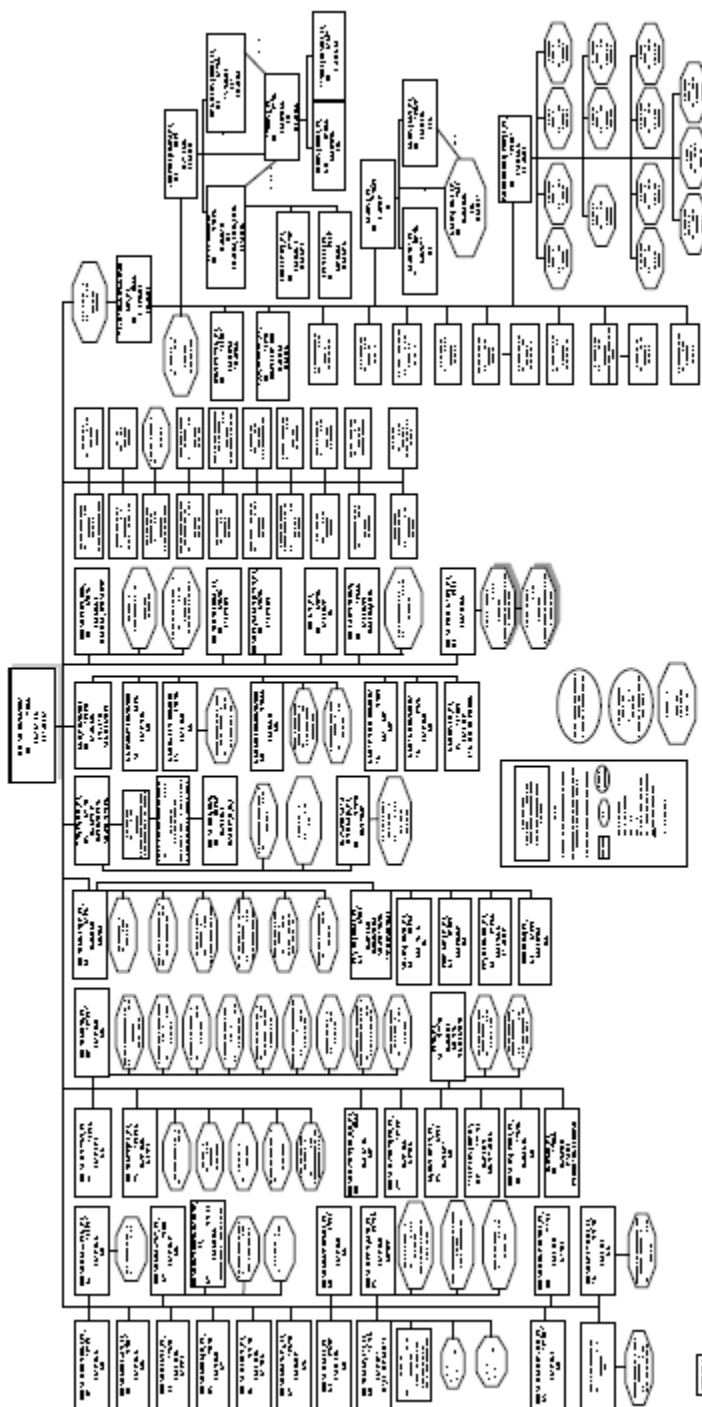
Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been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

By the Commission.

Decision and Order

EXHIBIT A

Rite Aid Corporation & Affiliates
Legal Counsel's Proposed Structure
As of 3/1/10



Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Rite Aid Corporation (“Rite Aid”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

The Commission’s proposed complaint alleges that Rite Aid is in the business of selling prescription and non-prescription medicines and supplies, as well as other products. It operates, among other things, approximately 4,900 retail pharmacy stores in the United States (collectively, “Rite Aid pharmacies”) and an online pharmacy business. The company allows consumers buying products in Rite Aid pharmacies to pay for their purchases with credit, debit and electronic benefit transfer cards; insurance cards; personal checks; or cash.

The complaint alleges that in conducting its business, Rite Aid routinely obtains information from or about its customers, including, but not limited to, name; telephone number; address; date of birth; bank account number; payment card account number and expiration date; prescription information, such as medication and dosage, prescribing physician name, address, and telephone number, health insurer name, and insurance account number and policy number; and Social Security number. The company also collects and maintains sensitive information from or about its employees and job applicants, which includes, among other things, Social Security numbers.

The complaint further alleges that Rite Aid engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive information from consumers, employees, and job applicants. In particular, Rite Aid

Analysis to Aid Public Comment

failed to: (1) implement policies and procedures to dispose securely of such information, including, but not limited to, policies and procedures to render the information unreadable in the course of disposal; (2) adequately train employees to dispose securely of such information; (3) use reasonable measures to assess compliance with its established policies and procedures for the disposal of such information; or (4) employ a reasonable process for discovering and remedying risks to such information.

The complaint alleges that as a result of these failures, Rite Aid pharmacies discarded materials containing sensitive information in clear readable text (such as pharmacy labels and job applications) in unsecured, publicly-accessible trash dumpsters on numerous occasions. For example, in July 2006 and continuing into 2007 and 2008, television stations and other media outlets reported finding such information in unsecured dumpsters used by Rite Aid pharmacies in at least 7 cities throughout the United States. When discarded in publicly-accessible dumpsters, such information can be obtained by individuals for purposes of identity theft or the theft of prescription medicines.

The proposed order applies to sensitive information about consumers, employees, and job applicants obtained by Rite Aid. It contains provisions designed to prevent Rite Aid from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits misrepresentations about the security, confidentiality, and integrity of sensitive information. Part II of the order requires Rite Aid to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of such information (whether in paper or electronic format) about consumers, employees, and those seeking to become employees. The order covers health and other sensitive information obtained by all Rite Aid entities, including, but not limited to, retail pharmacies. The security program must contain administrative, technical, and physical safeguards appropriate to Rite Aid's size and complexity, the nature and scope of its activities, and the sensitivity of the information collected from or about consumers and employees. Specifically, the order requires Rite Aid to:

Analysis to Aid Public Comment

- Designate an employee or employees to coordinate and be accountable for the information security program.
- Identify material internal and external risks to the security, confidentiality, and integrity of sensitive information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding sensitive information they receive from Rite Aid, and require service providers by contract to implement and maintain appropriate safeguards.
- Evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.

Part III of the proposed order requires Rite Aid to obtain within one year, and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of sensitive consumer, employee, and job applicant information has been protected.

Analysis to Aid Public Comment

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Rite Aid to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, Rite Aid must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Rite Aid submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part VIII is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The Commission conducted its investigation jointly with the Office for Civil Rights in the Department of Health and Human Services (“OCR-HHS”). Working together, the Commission and OCR-HHS each entered into separate but coordinated agreements with Rite Aid to resolve all the issues of both agencies.

This is the Commission’s twenty-ninth case to challenge the failure by a company to implement reasonable information security practices, and the second case: (1) involving a health provider, (2) proceeding jointly with OCR-HHS, and (3) challenging the security of employee data.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.

Complaint

IN THE MATTER OF

**PILOT CORPORATION, PROPELLER
CORPORATION, AND FLYING J INC.**

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATION OF
SEC. 7 OF THE CLAYTON ACT AND SEC. 5 OF THE FEDERAL TRADE
COMMISSION ACT

Docket No. C-4293; File No. 091 0125

Complaint, June 29, 2010 — Decision, November 15, 2010

The consent order addresses allegations that the acquisition by Pilot Corporation (“Pilot”) of Flying J Inc.’s travel center businesses would result in higher diesel fuel prices for long-haul trucking fleets. The consent order requires Pilot to divest the travel centers to Love’s Travel Stops and Country Stores (“Love’s”) and to provide Love’s access to and use of a fuel purchase card system that Pilot acquired; to continue operating Wendy’s restaurants affiliated with certain divested travel centers for one year; to provide Love’s with business information related to the travel centers being divested; and to maintain the travel centers as viable businesses pending divestiture. The consent order further permits the Commission to appoint a trustee to oversee the divestiture, if necessary.

Participants

For the *Commission*: Karen Kazmerzak, Mary N. Lehner, Justin Stewart-Teitelbaum, Terry Thomas, Cathlin Tully, and Josie M. Williams.

For the *Respondents*: Marimichael O. Skubel, Kirkland and Ellis LLP; and Rebecca Farrington and George L. Paul, White and Case LLP.

COMPLAINT

Pursuant to the provisions of the Federal Trade Commission Act, and by virtue of the authority vested in it by said Act, the Federal Trade Commission, having reason to believe that Respondents Pilot Corporation and Propeller Corp. (collectively, “Pilot”), and Flying J Inc. have entered into acquisition agreements which, if consummated, would violate Section 7 of the Clayton Act, as amended, 15 U.S.C. § 18, and Section 5 of the Federal Trade Commission Act, as amended, 15 U.S.C. § 45, and