Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Rite Aid Corporation, File No. 0723121

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 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:

- 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.

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.