0723121

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of **RITE AID CORPORATION,** **a corporation, and** **RITE AID HDQTRS. CORP.,** **a corporation.**	**DECISION AND ORDER** **DOCKET NO. C-4308**

DECISION

a. Rite Aid Corporation,

B. Security or Surveillance

2. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

3. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

4. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in English, Spanish, and each other language in which a Covered Business provides signage or other disclosures in the physical location or on the website where the disclosure appears.

5. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

6. The disclosure must not be contradicted or mitigated by, or inconsistent with, any other statements or representations in or near the disclosure.

7. When the deployment of an Automated Biometric Security or Surveillance System targets a specific group, such as children, the elderly, or the terminally

at group.

E. Covered Business means (1) any Respondent; (2) any business of which one or more Respondents is a majority owner or controls, directly or indirectly.

F.

pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

G.

including: (a) a first and last name; (b) a home or physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a

government-issued identification number; (f) date of birth; (g) geolocation information sufficient to identify street name and name of a city or town; (h) bank account information or credit or debit card information (including a partial credit or debit card number with more than five digits); (i) user identifier, or other persistent identifier that can be used to recognize a user over time and across different devices, websites, or online services; (j) user account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted); (k) Biometric Information; or (*l*) Health Information.

H. or Analysis ated Biometric Security or Surveillance System that analyzes or uses depictions or images, descriptions, recordings, copies, measurements, or geometry of or related to face to generate an Output.

I. Gallery list of samples of Biometric Information created and retained for purposes of comparison with other samples in connection with the use of an Automated Biometric Security or Surveillance System to generate an Output.

J. present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. It includes, but is not limited to, the following information relating to an individual: (a) prescription information, such as medication and dosage; (b) prescribing physician name, address, and telephone number; (c) health insurer name, insurance account number, or insurance policy number; (d) information concerning medical- or health-related purchases; and (e) any information that is derived or or pattern of activities, from which a determination is made that the individual has a health condition or is taking a drug.

K. Output an Output that is false, misleading, or incorrect and includes, to the extent that the Output of an Automated Biometric Security or Surveillance System is binary, (1) false positives or false acceptances and (2) false negatives or false rejections.

L. alert, prediction, analysis, assessment, determination, recommendation, identification, calculation, candidate list, or inference that is generated by a machine-based system processing Biometric Information.

M. contractor, service provider, or other agent of a Covered Business whose job duties include the operation or oversight of any aspect of an Automated Biometric Security or Surveillance System.

N. s mean Rite Aid Corporation, Rite Aid Hdqtrs Corp., and their subsidiaries, divisions, successors and assigns.

O. or Surveillance a purpose related to surveillance (including but Consent); the detection, deterrence, prediction, or investigation of theft, crime, fraud, or other misconduct; or access to locations, material goods, information, systems, or networks.

P.

permitted access to Covered Information from, by, or at the direction of a Covered Business through its provision of services directly to a Covered Business.

Provisions

I. Use of Facial Recognition or Analysis Systems Prohibited

IT IS ORDERED that Respondents, in connection with the activities of any Covered Business, are prohibited for five (5) years from the effective date of this Order from deploying or using, or assisting in the deployment or use of, any Facial Recognition or Analysis System, whether directly or through an intermediary, in any retail store or retail pharmacy or on any online retail platform.

II. Deletion of Covered Biometric Information

IT IS FURTHER ORDERED that Respondents; and Respondents employees; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, must, unless prohibited by law:

A. Within forty-five (45) days after the effective date of this Order, delete or destroy all photos and videos of consumers used or collected in connection with the operation of a Facial Recognition or Analysis System prior to the effective date of this Order, and any data, models, or algorithms derived in whole or in part therefrom, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed;

B. Within sixty (60) days after the effective date of this Order, Respondents must:

1. Identify all third parties, other than government entities, that received photos and videos of consumers used or collected in connection with the operation of a Facial Recognition or Analysis System prior to the effective date of this Order, and any data, models, or algorithms derived in whole or in part therefrom from any Covered Business, provide a copy of the Complaint and Order to all such identified third parties, notify all such identified third parties in writing that the Federal Trade Commission alleges that Respondents used that information in a manner that was unfair in violation of the FTC Act, and instruct all such identified third parties to delete all photos and videos of consumers used or collected in connection with the operation of a Facial Recognition or Analysis System prior to the effective date of this Order, and any data, models, or algorithms derived in whole or in part therefrom, and demand written confirmation of deletion

Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue

and

2. Provide all receipts of confirmation and any responses from third parties within ten (10) days of receipt to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must

III. Mandated Automated Biometric Security or Surveillance System Monitoring Program

IT IS FURTHER ORDERED that Respondents, in connection with the operation of any retail store or retail pharmacy or online retail platform by any Covered Business, must not use any Automated Biometric Security or Surveillance System in connection with Biometric Information collected from or about consumers of such retail store, retail pharmacy, or online retail platform, unless (1) use of the Automated Biometric Security or Surveillance System is not prohibited pursuant to Provision I of this Order entitled Use of Facial Recognition or Analysis Systems Prohibited; and (2) Respondents first establish and implement, and thereafter maintain, a comprehensive Automated Biometric Security or Surveillance System Monitoring Program Respondents must identify and address risks that operation of the Automated Biometric Security or Surveillance System will result, in whole or in part, in physicalAuu003FJETQ0 0 612 792 reW*nBT/TT0 12 TfB

1. The consequences for consumers of Inaccurate Outputs of the Automated Biometric Security or Surveillance System, including actions that Respondents or others intend to or may foreseeably take in whole or in part as a result of such Outputs;

2. Any testing relating to the rate or likelihood of Inaccurate Outputs, the extent to which such testing was conducted using reliable methodologies and under conditions similar to those in which the Automated Biometric Security or Surveillance System will operate, and the results of such testing;

3. Any factors that are likely to affect the accuracy of the type of Automated Biometric Security or Surveillance System deployed, such as any characteristics of Biometric Information, of the context or method in which Biometric Information is captured, or of individuals whose Biometric Information is used in connection with the Automated Biometric Security or Surveillance System (e.g., skin tone or language or dialect spoken), that would increase or decrease the likelihood that its use in connection with the Automated Biometric Security or Surveillance System would result in Inaccurate Outputs;

4. The extent to which the specific components of the Automated Biometric Security or Surveillance System as deployed, including the specific types and models of any devices or software, that any Covered Business uses or will use to capture, transmit, or store Biometric Information could affect the likelihood that the Automated Biometric Security or Surveillance System produces Inaccurate Outputs;

5.

5. Documentation and monitoring of the Automated Biometric Security or Surveillance uracy that Respondents have conducted pursuant to sub-

a. The sources and manner of collection of data that have been used to train or otherwise develop algorithmic components of the Automated Biometric Security or Surveillance System;

b. The extent to which the training data are materially similar to the Biometric Information that will be used in connection with deployment of the Automated Biometric Security or Surveillance System in light of factors that are known to affect the accuracy of the type of Automated Biometric Security or Surveillance System deployed; and

c. The makeup of any datasets that have been used to train or otherwise develop algorithmic components of the Automated Biometric Security or Surveillance System, including

12. The extent to which consumers are able to avoid the Automated Biometric Security or Surveillance System without losing access to

e. The requirements of this Order;

3. Documenting, for each Output, any
the Output is Inaccurate and any actions that Operators take in whole or in part because of the Output;

4. Periodically, and at least annually, reviewing actions taken by any Operators in response to Outputs, updating the content of training for Operators to address systemic Operator errors identified by periodic reviews, and, if there is reason to believe that
Security or Surveillance System increases risk to consumers, or if an Operator fails to comply with the requirements of this Order, terminating such

c. Periodically, and at least annually, reviewing the means by which Biometric Information to be used in connection with the Automated Biometric Security or Surveillance System is captured, including the extent to which any software or hardware used to collect Biometric Information is functioning properly and are consistently capturing samples of Biometric Information that meet the quality standards developed and implemented pursuant to sub-Provision III.D.6.a and are not otherwise contributing to the generation of Inaccurate Outputs; and

7. Conducting documented testing of the Automated Biometric Security or Surveillance System prior to deployment and at least once every twelve (12) months thereafter. Such testing must be conducted with the Affirmative Express Consent of individuals whose Biometric Information will be used for testing and must:

   a. Be conducted under conditions that materially replicate the conditions under which the Automated Biometric Security or Surveillance System is actually used, taking into account factors that affect the accuracy of the type of Automated Biometric Security or Surveillance System to be tested, the means by which Biometric Information to be used in connection with the Automated Biometric Security or Surveillance System is captured, and the roles of Operators;

   b. Determine the rate at which the Automated Biometric Security or Surveillance
   extent to which the Outputs can be verified using evidence or information other than an Output of an Automated Biometric Security or Surveillance System. For example, if an Output indicates the identity of an individual, the Output is verified if it is corroborated by a review of government-issued identification documents;

   c. Identify factors that cause or contribute to Inaccurate Outputs; and

   d. Assess and measure any statistically significant variation in the Automated Biometric Security or Surveillance
   depending on demographic characteristics of the consumers whose

distress, including in connection with communications of the Outputs to law enforcement or other third parties, taking into account the extent to which such harms are likely to disproportionately affect particular demographics of consumers based on race, ethnicity, gender, sex, age, or disability (alone or in combination);

F. Provide the written System Assessment and Program, and any evaluations thereof or updates thereto, to Respondents ng body or, if no such board or equivalent governing body exists, to a senior officer of Respondents responsible for the Program at least once every twelve (12) months; and

G. Not deploy or discontinue deployment of an Automated Biometric Security or Surveillance System if:

1. Respondents do not possess competent and reliable scientific evidence that is sufficient in quality and quantity based on standards generally accepted in the relevant scientific fields, when considered in light of the entire body of relevant and reliable scientific evidence, to substantiate that Outputs of the Automated Biometric Security or Surveillance System are likely to be accurate. For purposes of this Provision III, competent and reliable scientific evidence means tests, analyses, research, or studies that have been conducted and evaluated in an objective manner by qualified persons and are generally accepted in the profession to yield accurate and reliable results; or

2. Respondents have reason to believe, taking into account the System Assessment, the Program, all consumer complaints, and all monitoring, testing, documentation, and evaluations conducted pursuant to the Program, that:

a. Respondents Security or Surveillance System creates or contributes to a risk that Inaccurate Outputs will cause consumers to experience substantial physical, financial, or reputational injury, discrimination based on race, ethnicity, gender, sex, age, or disability, stigma, or severe emotional distress to consumers, including in connection with communications of the Outputs to law enforcement or other third parties, taking into account the extent to which such harms are likely to disproportionately affect consumers based on race, ethnicity, gender, sex, age, or disability; and

b. The identified risks are not substantially and timely eliminated by modifications to the Program.

IV. Mandatory Notice and Complaint Procedures for Automated Biometric Security or Surveillance Systems

IT IS FURTHER ORDERED that Respondents, for any Covered Business, in connection with the operation of any retail store or retail pharmacy or online retail platform,

must not use any Automated Biometric Security or Surveillance System in connection with Biometric Information collected from or about consumers of such retail store, retail pharmacy, or online retail platform, unless (1) use of the Automated Biometric Security or Surveillance System is not prohibited pursuant to Provision I of this Order entitled Use of Facial Recognition or Analysis Systems Prohibited and (2) Respondents, prior to implementing any such Automated Biometric Security or Surveillance System, establish and implement, and thereafter maintain, procedures to provide consumers with notice and a means of submitting complaints related to Outputs of the Automated Biometric Security or Surveillance System. Specifically, Respondents must:

A. Provide written notice to all consumers who will have their Biometric Information enrolled in any Gallery used in conjunction with an Automated Biometric Security or Surveillance System, unless Respondents are unable to provide the notice due to safety concerns or the nature of a security incident that forms the basis for enrollment. Respondents shall provide such notice prior to or promptly after enrollment, and the notice shall include:

    1. An explanation for the reasonable basis (as described in sub-Provision III.D.5) for enrollment in the Gallery, including a description of any security incident that provided that basis;

    2. Instructions about how to obtain a copy of the sample of Biometric Information that was collected in order to enroll the consumer, which Respondents must make available upon request so long as Respondents retain said sample;

    3. The length of time for which Re

Thed sample

3. An explanation of how that action relates to the Output; and

4. An email address, online form, mailing address, and telephone number to which consumers can direct complaints or inquiries about the Output; the Automated Biometric Security or Surveillance System that generated the Output; or the use, sharing, or retention of their Biometric Information.

C. Investigate each complaint to (1) determine whether the relevant Output was an Inaccurate Output, and, if so, identify any factors that likely contributed to the generation of an Inaccurate Output; and (2) assess whether Operators responded to the Output in a manner that was appropriate and consistent with the requirements of this Order; and

D. Respond to each consumer complaint relating to the Automated Biometric Security or Surveillance System by:

1. Within seven (7) days of receiving the complaint, providing written confirmation of receipt to the consumer who submitted the complaint. Such written confirmation should be provided using the same means of communication that the consumer used to submit the complaint, Q Inaoconfirma nBT/TT0 to submit the compWit

previous five (5) years, and precludes retention beyond what is reasonably necessary to achieve the purpose or purposes and serve the business needs for which it was collected; and

C. The basis for the timeframe for deletion

B. Respondents privacy and security measures to honor the privacy choices exercised by consumers;

C. Respondents collection, maintenance, use, disclosure, or deletion of Covered Information; or

D. The extent to which Respondents make or have made Covered Information accessible to any third parties.

VIII. Mandated Information Security Program for Covered Businesses

IT IS FURTHER ORDERED that Respondents, for any Covered Business, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must each, within 90 days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive information security program

Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Provide the written Information Security Programs and any evaluations thereof or updates thereto to the of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the

Covered Information identified in response to sub-Provision D of this Provision. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, alteration, destruction, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Training of all employees, at least once every twelve (12) months, on how to safeguard Covered Information including, for information security personnel, security updates and training sufficient to address relevant security risks, and verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures;

material change, the Covered Business must obtain or possess new documentation aterial to the security of Covered Information within the possession, custody, or control of the Covered Business;

M. Maintain in one or more central repositories all documentation about or provided by each Vendor pursuant to sub-Provisions J, K, and L of this Provision, including but not limited to each contract with a Vendor, for a period of five (5) years from when it was obtained or provided. This sub-Provision is in addition to and not in lieu of the Provision entitled Recordkeeping;

N. At least once every twenty-four (24) months, and promptly following a Covered Incident affecting 100 or more consumers involving a Vendor or determination of a material change under sub-Provision L of this Provision, conduct written reassessments of each Vendor (or, in the case of a Covered Incident affecting 100 or more consumers, each relevant Vendor) to determine the continued adequacy of their safeguards to control the internal and external risks to the security of Covered

assessment for each Vendor should be commensurate with the risk it poses to the security of Covered Information; and

O. Maintain in one or more central repositories all documentation created by the Covered Business pursuant to sub-Provision N of this Provision for a period of five (5) years from when it was created. This sub-Provision is in addition to and not in lieu of the Provision entitled Recordkeeping.

IX. Third Party Information Security Assessments for Covered Businesses

IT IS FURTHER ORDERED that Respondents must obtain initial and biennial

A. The Assessments must be obtained from a qualified, objective, independent third-party

the profession; (2) conducts an independent review of the Information Security Program; and (3) retains all documents relevant to each Assessment for 5 years after completion of such Assessment and will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Respondents must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in their sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the Mandated Information Security Program for Covered Businesses required by Provision VIII of this Order has been put in place for the initial Assessment; and (2) each two-year period thereafter for 20 years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period:

1. Determine whether Respondents have implemented and maintained the Information Security Program required by the Provision entitled Mandated Information Security Program for Covered Businesses;

2. Assess the effectiveness of Respondents implementation and maintenance of sub-Provisions A-O of the Provision entitled Mandated Information Security Program for Covered Businesses;

3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;

4. Address the status of gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and

5. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of the ty, and risk profile; and (b) sufficient to justify the

assertions or attestations by Respondents management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondents management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent any Respondent revises, updates, or adds one or more safeguards required under the Provision entitled Mandated Information Security Program for Covered Businesses in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondents must submit an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure of the initial Assessment to the Commission within 10 days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to:

Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line *In re Rite Aid Corporation*, FTC File No. C- s must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable for public disclosure until the Order is terminated and must provide each such Assessment to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right- Information Security Program Assessment

X. Cooperation with Third-Party Information Security Assessor

IT IS FURTHER ORDERED that, Respondents, whether acting directly or indirectly, in connection with any Assessment required by the Provision entitled Third Party Information Security Assessments for Covered Businesses must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondents networks and all of Respondents information technology assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the networks and information technology assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly

Respondents have implemented and maintained the Mandated Information Security Program for Covered Businesses; (2) assessment of the effectiveness of the Respondents implementation and maintenance of sub-Provisions A-O of the required Mandated Information Security Program for Covered Businesses; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Mandated

XI. Annual Certification

IT IS FUTT0 1279 re*nBT7TT2 aE Rm BT ORat

Information Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business is not aware of any material

XIII. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

A. Each Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order.

B. For twenty (20) years after the issuance date of this Order, each Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and trol, or operate one or more stores or online retail platforms; (3) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (4) any business entity resulting from any change in structure as set forth in the Provision entitled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondents delivered a copy of this Order, Respondents must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XIV. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with
their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business; (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission;

B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in (a) any designated point of contact; or (b) the

plans, test results, reports, studies, reviews, audits, policies, training materials, and

Provisions of this Order, for the compliance period covered by such System Assessment;

F. A copy of each widely disseminated and materially different representation by Defendants that describes the extent to which Defendants maintains or protects the privacy, security, availability, confidentiality, or integrity of any Covered Information, including

representatives as consumers, suppliers, or other individuals or entities, to Respondents or