

Exhibit A

[Proposed] Stipulated Order for Permanent
Injunction and Other Relief

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. Venue is proper as to all parties in this District.
3. The Complaint charges Defendants with unfair acts or practices in violation of Sections 5(a) and 5(n) of the FTC Act, 15 U.S.C. §§ 45(a), (n), in connection with their (1) facial recognition technology practices and (2) failure to implement or maintain a comprehensive information security program in violation of Part II of the Commission’s Decision and Order in *In re Rite Aid Corporation*, C-4308, 150 F.T.C. 694 (Nov. 12, 2010) (“2010 Decision and Order”). Defendants are thus subject to relief under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b).
4. Defendants waive any claim that they may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Stipulated Order and the Decision and Order set forth in Attachment A, and agree to bear their own costs and attorney fees.
5. Defendants neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Stipulated Order or in the Decision and Order set forth in Attachment A. Only for purposes of this action, Defendants admit the facts necessary to establish jurisdiction.
6. Defendants and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Stipulated Order or the Decision and Order set forth in Attachment A.
7. The Plaintiff’s commencement and prosecution of this action are actions to enforce the Plaintiff’s police or regulatory power. As a result, if the Bankruptcy Cases are

pending as of the date of entry of this Order, these actions are excepted from the automatic stay pursuant to 11 U.S.C. § 362(b)(4).

DEFINITIONS

“**Defendant(s)**” means Rite Aid Corporation, Rite Aid Hdqtrs Corp., and all of their subsidiaries, divisions, successors and assigns, individually, collectively, or in any combination.

I. ORDERS OF BANKRUPTCY COURT

IT IS FURTHER ORDERED that this Order does not restrain or enjoin the deposit, exchange, distribution, investment, or withdrawal of assets owned or held by Defendants and being administered in accordance with the United States Bankruptcy Code and orders of the Court in the Bankruptcy Cases. For the avoidance of doubt this Stipulated Order does not create a contingent liability against the Defendants and does not preclude the full distribution of assets held by the Defendants in the Bankruptcy Cases.

II. MODIFICATION OF 2010 DECISION AND ORDER

IT IS FURTHER ORDERED that Defendants: (i) consent to reopening of the proceeding in FTC Docket No. C-4308; (ii) waive their rights under the show cause procedures set forth in Section 3.72(b) of the Commission’s Rules of Practice, 16 C.F.R. § 3.72(b); and (iii) consent to modification of the 2010 Decision and Order in *In re Rite Aid Corporation*, C-4308, 150 F.T.C. 694 (Nov. 12, 2010), with the Commission order in Attachment A, which shall replace and supersede the 2010 Order.

III. CONTINUING JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction in this matter for purposes of construction, modification, and enforcement of this Stipulated Order.

SO ORDERED this ____ day of _____ 202__.

UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

Dated: December 19, 2023


FOR THE FEDERAL TRADE COMMISSION

JAMES A. KOHM
Associate Director
Division of Enforcement

BENJAMIN WISEMAN
Associate Director
Division of Privacy and Identity Protection

LAURA KOSS
Assistant Director
Division of Enforcement

TIFFANY GEORGE
Assistant Director
Division of Privacy and Identity Protection


CHRISTOPHER J. ERICKSON
Attorney
Division of Enforcement

/s/ Robin L. Wetherill
ROBIN WETHERILL
Attorney
Division of Privacy and Identity Protection

BRIAN M. WELKE
Attorney
Division of Enforcement

LEAH FRAZIER
Attorney
Division of Privacy and Identity Protection

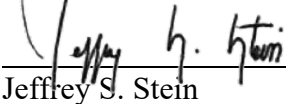
Federal Trade Commission
600 Pennsylvania Avenue,
N.W. Mail Stop CC-6316
Washington, D.C. 20580
(202) 326-3671 (Erickson); - 2897 (Welke)
cerickson@ftc.gov; bwelke@ftc.gov

N. DIANA CHANG
Attorney
Division of Privacy and Identity Protection

Federal Trade Commission
600 Pennsylvania Avenue,
N.W. Mail Stop CC-6316
Washington, D.C. 20580
(202) 326-2220 (Wetherill); - 2187
(Frazier); (415) 848-5100 (Chang)
rwetherill@ftc.gov; lfrazier@ftc.gov;
nchang@ftc.gov

Dated: December 13, 2023

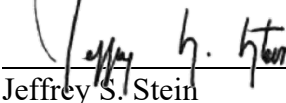
**FOR DEFENDANT RITE AID
CORPORATION**



Jeffrey S. Stein
Chief Executive Officer
Rite Aid Corporation

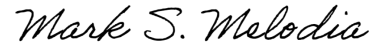
Dated: December 13, 2023

**FOR DEFENDANT RITE AID HDQTRS.
CORP.**



Jeffrey S. Stein
Chief Executive Officer
Rite Aid Hdqtrs. Corp.

Dated: December 14, 2023



ANTHONY E. DIRESTA
MARK S. MELODIA
Holland & Knight LLP
800 17th Street N.W.
Suite 1100
Washington, D.C. 20006
(202) 955-3000
Anthony.DiResta@hklaw.com
Mark.Melodia@hklaw.com

RICHARD H. CUNNINGHAM
Kirkland & Ellis LLP
1301 Pennsylvania Ave. N.W.
Washington D.C. 20004
(202) 389-3119
Richard.Cunningham@kirkland.com

ALLISON W. BUCHNER
Kirkland & Ellis LLP
2049 Century Park East, Suite 3700
Los Angeles, CA 90067
(310) 552-4302
Allison.Buchner@kirkland.com

*Counsel for Defendants Rite Aid Corporation and
Rite Aid Hdqtrs. Corp.*

Attachment A

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

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of Respondents named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondents a draft Complaint. BCP proposed presenting the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act, 15 U.S.C. §§ 45(a), (n), and 53(b), including by violating the Commission’s 2010 Decision and Order in the above-captioned matter.

Respondents neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order. For purposes of this action only, Respondents admit the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act and the Decision and Order the Commission previously issued in *In re Rite Aid Corporation*, C-4308, 150 F.T.C. 694 (Nov. 12, 2010), and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:

- a. Rite Aid Corporation, a Delaware corporation with its principal office or place of business at 1200 Intrepid Avenue, 2nd Floor, Philadelphia, PA 17011; and
 - b. Rite Aid Hdqtrs. Corp., a Delaware corporation with its principal office or place of business at 1200 Intrepid Avenue, 2nd Floor, Philadelphia, PA 17011.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.
 3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, including by violating Provision II of an order previously issued by the Commission.
 4. Respondents waive any claim that they may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agree to bear its own costs and attorney fees.
 5. Respondents and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

- A. “Affirmative Express Consent” means any freely given, specific, informed, and unambiguous indication of an individual consumer’s wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual of: (i) the categories of information that will be collected; (ii) the specific purpose(s) for which the information is being collected; (iii) the names or categories of Third Parties collecting the information, or to whom the information is disclosed, provided that if Respondent discloses the categories of Third Parties, the disclosure shall include a hyperlink or information about how to access a separate page listing the names of the Third Parties; (iv) a simple, easily-located means by which the consumer can withdraw consent; and (v) any limitations on the consumer’s ability to withdraw consent. The Clear and Conspicuous disclosure must be separate and apart from any “privacy policy,” “terms of service,” “terms of use,” or other similar document, but it may reference them.

The following do not constitute Affirmative Express Consent:

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or
2. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.

- B. “Automated Biometric Security or Surveillance System” means any machine-based system, including any computer software, application, or algorithm, that analyzes or uses Biometric Information of, from, or about individual consumers to generate an Output that relates to those consumers, notwithstanding any assistance by a human being in such analysis or use, and that is used in whole or in part for a Security or Surveillance Purpose. *Provided, however,* that the term “Automated Biometric or Surveillance Security System” as used in this Order does not include:
1. A camera or similar sensor that is used to capture images or videos of individuals that are not collected or used in connection with the generation of an Output;
 2. Any system to the extent that it is used to authenticate or identify Respondents’ employees, contractors, or agents in connection with the performance of their job duties, so long as Respondents receive Affirmative Express Consent for the collection and use of any Biometric Information in connection with such authentication; and
 3. Any system to the extent it is used exclusively in the direct provision of medical services by or under the supervision of a physician, registered nurse, pharmacist, or other licensed health care professional, so long as Respondents receive Affirmative Express Consent for the collection and use of any Biometric Information in connection with such system.
- C. “Biometric Information” means data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person’s body, including depictions or images, descriptions, recordings, or copies of an individual’s facial or other physical features (e.g., iris/retina scans), finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern). “Biometric Information” does not include data that relates solely to user accounts or credentials, such as a username, or to user devices, such as device IDs or IP addresses, in isolation from data that depict or describe or are used to infer physical, biological, or behavioral traits, characteristics, or measurements of or relating to a person’s body.
- D. “Clear(ly) and Conspicuous(ly)” means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
1. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

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 ill, “ordinary consumers” includes reasonable members of that 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. “Covered Incident” means any incident that results in a Covered Business notifying, 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. “Covered Information” means information from or about an individual consumer, 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 screen name; (d) a mobile or other telephone number; (e) a driver’s license or other 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. “Facial Recognition or Analysis System” means an Automated Biometric Security or Surveillance System that analyzes or uses depictions or images, descriptions, recordings, copies, measurements, or geometry of or related to an individual’s face to generate an Output.
- I. “Gallery” means a collection, database, or 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. “Health Information” means individually identifiable information relating to the past, 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 extrapolated from information about an individual’s activities, or pattern of activities, from which a determination is made that the individual has a health condition or is taking a drug.
- K. “Inaccurate Output” means 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. “Output” means a match, alert, prediction, analysis, assessment, determination, recommendation, identification, calculation, candidate list, or inference that is generated by a machine-based system processing Biometric Information.
- M. “Operator” means an officer, employee, manager, 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. “Respondents” mean Rite Aid Corporation, Rite Aid Hdqtrs Corp., and their subsidiaries, divisions, successors and assigns.
- O. “Security or Surveillance Purpose” means a purpose related to surveillance (including but not limited to tracking individuals’ location or behavior without Affirmative Express 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. “Vendor” means any person or entity that receives, maintains, processes, or otherwise is 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’ officers, agents, and 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. Defendant’s instruction to each such identified third party shall include a description of the Biometric Information to be deleted. Defendant must provide all instructions sent to the identified third parties 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 begin: “In the Matter of Rite Aid;” 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 begin: “In the Matter of Rite Aid.”

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 (the “Program”). In establishing, implementing, and maintaining the 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 physical, financial, or reputational harm to consumers, stigma, or severe emotional distress, including in connection with communications of the Outputs to law enforcement or other third parties, and must also identify and address risks that any such harms will disproportionately affect consumers based on race, ethnicity, gender, sex, age, or disability, alone or in combination. To satisfy this requirement, Respondents must:

- A. Document in writing the content, implementation, and maintenance of the Program;
- B. Designate a qualified employee or employees to coordinate and be responsible for the Program;
- C. For each Automated Biometric Security or Surveillance System used, prior to its implementation (or for any Automated Biometric Security or Surveillance System in use as of the effective date of this Order, within ninety (90) days of the effective date of this Order) and, thereafter, at least once every twelve (12) months, conduct a written assessment (“System Assessment”) of potential risks to consumers from the use of the Automated Biometric Security or Surveillance System, including, at a minimum, risks that consumers could experience physical, financial, or reputational injury, stigma, or severe emotional distress in connection with Inaccurate Outputs of the Automated Biometric Security or Surveillance System (e.g., if the technology misidentifies a consumer). The System Assessment must include a review of:

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. Documentation and monitoring of the Automated Biometric Security or Surveillance System's accuracy that Respondents have conducted pursuant to sub-Provision III.D;
6. The extent to which the Automated Biometric Security or Surveillance System was developed to be used for a similar purpose and under similar conditions to those under which any Covered Business deploys or will deploy the Automated Biometric Security or Surveillance System;
7. The methods by which any algorithms comprising part of the Automated Biometric Security or Surveillance System were developed, including the extent to which such components were developed using machine learning or any other method that entails the use of datasets to train algorithms, and the extent to which these methods increase the likelihood that Inaccurate Outputs will occur or will disproportionately affect consumers depending on their race, ethnicity, gender, sex, age, or disability status. This review should include, at a minimum:

- 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 the extent to which the datasets have been representative, in terms of race, ethnicity, gender, sex, age, and disability status, of the population(s) of consumers whose Biometric Information will be used in connection with deployment of the Automated Biometric Security or Surveillance System;
8. The context in which the Automated Biometric Security or Surveillance System is or will be deployed, including the geographical locations of stores deploying the technology, demographic characteristics, including race and ethnicity, of areas surrounding stores where technology is deployed, physical location within stores or sections of stores, such as pharmacies, of system components, and the scale, timing and duration of the deployment (e.g., how long the system will be deployed and whether the system will operate continuously or only under certain circumstances);
 9. All policies and procedures governing the operation of the Automated Biometric Security or Surveillance System and its software, algorithms, hardware, or other components;
 10. The extent to which Operators receive sufficient and relevant training or are subject to oversight;
 11. The extent to which the Automated Biometric Security or Surveillance System is likely to generate Inaccurate Outputs at a higher rate when analyzing or using Biometric Information collected from or about consumers of particular races, ethnicities, sexes, genders, ages, or who have disabilities (or any of these categories in combination), taking into account technical elements of the Automated Biometric Security or Surveillance System and any components thereof, the selection of locations in which to deploy the Automated Biometric Security or Surveillance System, and the context or manner in which any Covered Business has deployed or will deploy the Automated Biometric Security or Surveillance System; and

12. The extent to which consumers are able to avoid the Automated Biometric Security or Surveillance System without losing access to any Covered Business's physical retail locations or online services, including by withholding Affirmative Express Consent for, or opting out of, the collection or use of their Biometric Information.

D. Implement, maintain, and document safeguards that are designed to control for the risks Respondents identify in the System Assessment. Each safeguard must be based on the severity of the risk to consumers and the likelihood that the risk could be realized. Such safeguards must also include:

1. Selecting and retaining service providers with duties related to the subject matter of this Order that are capable of performing those duties in a manner consistent with the Program and this Order, and contractually requiring such service providers to (1) comply with the requirements of the Program and this Order and (2) make available to Respondents all information and materials necessary to conduct the System Assessment;
2. Requiring and documenting regular and at least annual training for all Operators, which must cover, at a minimum:
 - a. Methodologies for interpreting or assessing the validity of the Outputs of the Automated Biometric Security or Surveillance System, including for judging whether Outputs are Inaccurate;
 - b. Evaluation of Biometric Information to determine its quality, value, and appropriateness for use in connection with the Automated Biometric Security or Surveillance System, particularly in light of each relevant factor identified pursuant to sub-Provision III.C.3 and the quality standards implemented pursuant to sub-Provision III.D.6.a;
 - c. An overview of the types of human cognitive bias, such as automation bias and confirmation bias, that could foreseeably affect Operators' interpretations of the Outputs;
 - d. Known limitations of the Automated Biometric Security or Surveillance System, including factors that are known to affect the accuracy of the Outputs of Automated Biometric Security or Surveillance Systems of the type deployed, such as image or sound quality, the method by which Biometric Information to be used in connection with the Automated Biometric Security or Surveillance System is collected, background images or sounds, the passage of time since the capture of a Biometric Information sample, or relevant demographic, physical, or other traits of the individual to whom Biometric Information pertains (such as race, ethnicity, sex, gender, age, or disability, alone or in combination); and

- e. The requirements of this Order;
3. Documenting, for each Output, any Respondent's determination of whether 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 an Operator's operation of the Automated Biometric Security or Surveillance System increases risk to consumers, or if an Operator fails to comply with the requirements of this Order, terminating such Operator's operation of the Automated Biometric Security or Surveillance System;
 5. Developing, implementing, and maintaining policies and procedures designed to ensure that Respondents have a reasonable basis for enrolling each consumer's Biometric Information in any Gallery;
 6. Implementing and maintaining policies and procedures to ensure that samples of Biometric Information used in connection with the Automated Biometric Security or Surveillance System do not increase the likelihood of Inaccurate Outputs, including by:
 - a. Developing, implementing, and enforcing written quality standards for Biometric Information to be used in connection with the Automated Biometric Security or Surveillance System, taking into account the nature of the Automated Biometric Security or Surveillance System, the manner in which the Biometric Information is captured, and characteristics of Biometric Information that could affect the accuracy of the Automated Biometric Security or Surveillance System;
 - b. To the extent that deployment of the Automated Biometric Security or Surveillance System entails the creation of a Gallery, periodically, and at least monthly, reviewing such Gallery to identify and, as soon as practicable, remove samples of Biometric Information that (1) have been associated with two or more Inaccurate Outputs, including Outputs that were determined to be Inaccurate based on investigations conducted in response to consumer complaints pursuant to sub-Provision IV.C of this Order; (2) do not meet the quality standards referenced in sub-Provision III.D.6.a; (3) are required to be deleted pursuant to Provision V of this Order, entitled "Required Retention Limits for Biometric Information;" or (4) have been enrolled without a reasonable basis or in violation of policies and procedures implemented pursuant to sub-Provision III.D.5;

- 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 System's Outputs are Inaccurate, including by assessing the 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 System's rate of Inaccurate Outputs depending on demographic characteristics of the consumers whose Biometric Information is analyzed or used, such as race, ethnicity, sex, gender, age, or disability (alone or in combination).
- E. Evaluate and adjust the Program in light of any circumstance that Respondents know or have reason to know may materially affect the Program's effectiveness. At a minimum, every twelve (12) months, each Covered Business must evaluate the effectiveness of the Program in light of the System Assessment and the results of all monitoring, testing, and documentation conducted pursuant to the Program. Respondents must implement modifications to substantially and timely remediate any identified risks that consumers may experience physical, financial, or reputational injury, stigma, or severe emotional

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' board of directors or governing 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' use of the Automated Biometric 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 Respondent will retain the consumer's Biometric Information in the Gallery; and
 4. An email address, online form, mailing address, and telephone number to which consumers can direct complaints or inquiries about their enrollment in the Gallery; the Automated Biometric Security or Surveillance System; or retention of their Biometric Information.

- B. Provide written notice to all consumers with respect to whom Respondents, in connection with an Output, take an action that could result in physical, financial, or reputational harm to the consumers, including in connection with communications of the Output to law enforcement or other third parties, unless Respondents are unable to provide the notice due to safety concerns or the nature of a security incident relating to the Output. Respondents shall provide such notice prior to taking, or, if prior notice is infeasible, at the time of taking an action, and the notice shall include:
 1. The date, approximate time, and location of the Output;
 2. A description of the action or actions taken;

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, or by another means selected by the consumer during the complaint submission process, and should state that Respondents will investigate the consumer's complaint and provide its conclusions within thirty (30) days;
 2. Within thirty (30) days of providing the written confirmation, providing a written response to the consumer who submitted the complaint. Such written response must be provided using the same means of communication as the written confirmation and must (1) state whether the Output was determined to be an Inaccurate Output and the basis for such a determination; and (2) describe in general terms actions taken in response to the complaint.

V. Required Retention Limits for Biometric Information

IT IS FURTHER ORDERED that Respondent, for any Covered Business, in connection with the operation of any retail store, retail pharmacy, or online retail platform must, prior to implementing any Automated Biometric Security or Surveillance System, develop and implement, for each type of Biometric Information from or about consumers of such physical retail location or online retail platform that is collected in whole or in part for use in connection with any Automated Biometric Security or Surveillance System, a written retention schedule setting forth:

- A. All purposes and business needs for which the Covered Business collects or uses the type of Biometric Information;
- B. A timeframe for deletion of the Biometric Information that is no greater than five (5) years, except to the extent that retention beyond five years is required by law or Respondents have obtained Affirmative Express Consent for the retention within the

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 of the Biometric Information, including any foreseeable effect on the likelihood of Inaccurate Outputs of the passage of time since a given sample of the type of Biometric Information was collected or enrolled in a Gallery.

VI. Disclosure of 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, retail pharmacy, or online retail platform, must, within thirty (30) days after the effective date of this Order, post Clear and Conspicuous notices disclosing the Covered Business's use of any Automated Biometric Security or Surveillance System in connection with Biometric Information collected from or about consumers of the physical retail location or online retail platform. Such notices must be posted in each physical retail location, and on each website, mobile application, or online service on or through which Biometric Information from or about consumers is collected or used in whole or in part for the purpose of operating an Automated Biometric Security or Surveillance System, and must include, as to each such location, website, mobile application, or online service:

- A. The specific types of Biometric Information that are collected in whole or in part for the purpose of operating an Automated Biometric Security or Surveillance System;
- B. The types of Outputs that are generated by the Automated Biometric Security or Surveillance Systems;
- C. All purposes for which the Covered Business uses each Automated Biometric Security or Surveillance System or its Outputs, including actions that the Covered Business may take on the basis of Outputs; and
- D. The timeframe for deletion of each type of Biometric Information used, as established pursuant to Provision V of this Order, entitled "Required Retention Limits for Biometric Information."

VII. Prohibition Against Misrepresentations

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication, the extent to which Respondents maintain and protect the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

- A. Respondents' privacy and security measures to prevent unauthorized access to Covered Information;

- 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 ("Information Security Program") that protects the security, confidentiality, and integrity of such 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 Program and any evaluations thereof or updates thereto to the Covered Business' board 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 Business's Information Security Program at least once every twelve (12) months and promptly (not to exceed 30 days) after a Covered Incident affecting 500 or more consumers;
- C. Designate a qualified employee or employees, who report(s) directly to the Executive Leadership Team (including the Chief Executive Officer, Chief Information Officer, and Chief Legal Officer) to coordinate and be responsible for the Information Security Program and keep the Executive Leadership Team and Board of Directors informed of the Information Security Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;
- D. Assess and document, at least once every twelve (12) months and promptly (not to exceed 30 days) following a Covered Incident affecting 100 or more consumers, internal and external risks to the security, confidentiality, or integrity of Covered Information that could 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;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks Covered Businesses identify to the security, confidentiality, or integrity of

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;
2. Documenting in writing the content, implementation, and maintenance of an incident response plan designed to ensure the identification of, investigation of, and response to the unauthorized access to Covered Information. Respondents shall revise and update this incident response plan to adapt to material changes to their assets or networks;
3. Implementing technical measures to log and monitor all networks and assets for anomalous activity and active threats. Such measures shall require Respondents to determine baseline system activity and identify and respond to anomalous events and unauthorized attempts to access or exfiltrate Covered Information;
4. Policies and procedures to minimize data collection, storage, and retention, including data deletion or retention policies and procedures;
5. Implementing data access controls for all assets (including databases) storing Covered Information and technical measures, policies, and procedures to minimize or prevent online attacks resulting from the misuse of valid credentials, including: (a) restricting inbound and outbound connections; (b) requiring and enforcing strong passwords or other credentials; (c) preventing the reuse of known compromised credentials to access Covered Information; (d) implementing automatic password resets for known compromised credentials; and (e) limiting employee access to what is needed to perform that employee's job function;
6. Requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all employees, contractors, and affiliates should not include telephone or SMS-based authentication methods and must be resistant to phishing attacks. Respondents may use equivalent, widely adopted industry authentication options that are not multi-factor, if the person responsible for the Information

Security Program under sub-Provision C of this Provision: (1) approves in writing the use of such equivalent authentication options; and (2) documents a written explanation of how the authentication options are widely adopted and at least equivalent to the security provided by multi-factor authentication;

7. Developing and implementing configuration standards to harden system components against known threats and vulnerabilities. New system components shall not be granted access to any Covered Businesses' network, resources, or Covered Information until they meet Respondents' configuration standards;
 8. Encryption of, at a minimum, all Social Security numbers, passport numbers, financial account information, tax information, dates of birth associated with a user's account, Health Information, and user account credentials while in transit or at rest on each Covered Businesses' computer networks, including but not limited to cloud storage;
 9. Policies and procedures to ensure that all networks, systems, and assets with access to Covered Information within the Covered Businesses' custody or control are securely installed and inventoried at least once every twelve (12) months;
 10. Implementing vulnerability and patch management measures, policies, and procedures that (a) require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed and (b) include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated; and
 11. Enforcing policies and procedures to ensure the timely investigation of data security events and the timely remediation of critical and high-risk security vulnerabilities.
- F. Assess, at least once every twelve (12) months and promptly (not to exceed 30 days) following a Covered Incident affecting 100 or more consumers, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Covered Information, and modify the Information Security Program based on the results;
- G. Test and monitor the effectiveness of the safeguards in place at least once every twelve (12) months and promptly (not to exceed 30 days) following a Covered Incident affecting 100 or more consumers, and modify the Information Security Program based on the results as necessary. Such testing and monitoring must include: (1) vulnerability testing of each Covered Business' network and applications once every four (4) months and promptly (not to exceed 30 days) after a Covered Incident; and (2) penetration testing of each Covered Business' network(s) and applications at least once every twelve (12) months and promptly (not to exceed 30 days) after a Covered Incident;

- H. Evaluate and adjust the Information Security Program in light of any material changes to a Covered Business' operations or business arrangements, a Covered Incident affecting 100 or more consumers, new or more efficient technological or operational methods to control for the risks identified in sub-Provision D of this Provision, or any other circumstances that a Covered Business or its officers, agents, or employees know or have reason to know may have a material impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, each Covered Business must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program, if appropriate, based on the results;
- I. Select and retain Vendors capable of safeguarding Covered Information they access through or receive from each Covered Business, including by implementing and maintaining a uniform process that is fully documented in writing to conduct risk assessments for each Vendor, and contractually require Vendors to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information. The uniform process must include a review and analysis of the information and documentation obtained about each Vendor pursuant to this Provision. The level of the assessment for each Vendor should be commensurate with the risk it poses to the security of Covered Information;
- J. Require each Vendor agree by contract (upon renewal or new engagement or, in any event, within 180 days of the effective date of this Order) to:
 - 1. Develop and implement policies and procedures for the prompt remediation and investigation of any incident that results in the Vendor or Covered Business notifying, pursuant to an applicable 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; and
 - 2. Notify the Covered Business in writing as soon as possible, and in any event no later than seventy-two (72) hours, if the Vendor has reason to believe that any person has accessed, exfiltrated, or otherwise obtained without authorization Covered Information that the Vendor obtained from the Covered Business.
- K. Obtain or possess for each Vendor, within 180 days of the effective date of this Order, documentation regarding the Vendor's information security program that is material to the security of Covered Information within the possession, custody, or control of the Covered Business, including, without limitation, documentation of the Vendor's cybersecurity risk assessment conducted within the last twelve (12) months. The Covered Business must be in possession of such documentation before it provides the Vendor with access to Covered Information;
- L. Determine in writing, at least once every twenty-four (24) months, whether there has been a material change to the Vendor's information security program. If there has been a

material change, the Covered Business must obtain or possess new documentation regarding the Vendor's information security program that is material 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 to a Vendor's information security program 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 Information and document the basis for the Covered Business's determination as to whether each Vendor's safeguards are adequate. The level of the 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 assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in 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 business's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on 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 must begin, “*In re Rite Aid Corporation*, FTC File No. C-4308.” Respondents 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-hand corner of each page, with the words “Information Security Program Assessment” in red lettering.

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 or by implication, any fact material to the Assessor’s: (1) determination of whether 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 Information Security Program for Covered Businesses.

XI. Annual Certification

IT IS FURTHER ORDERED that Respondents must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from Corporate Respondents’ Chief Executive Officer, _____, or if Mr./Ms. _____ no longer serves as Respondents’ Chief Executive Officer, President, or such other officer (regardless of title) that is designated in that Respondent’s Bylaws or resolution of the Board of Directors as having the duties of the principal executive officer of Respondent, then a senior corporate manager, or, if no such senior corporate manager exists, a senior officer responsible for Respondents’

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 noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents affecting 100 or more consumers that Respondents verified or confirmed during the certified period. The certification must be based on the personal knowledge of Mr./Ms. _____, the senior corporate manager, senior officer, or subject matter experts upon whom Mr./Ms. _____, the senior corporate manager, or senior officer reasonably relies in making the certification.

- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order 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 must begin, “*In re Rite Aid Corporation*, FTC File No. C-4308.”

XII. Covered Incident Reports

IT IS FURTHER ORDERED that, within 10 days of any notification to a United States federal, state, or local entity of a Covered Incident affecting 500 or more consumers, Respondents, for any Covered Business, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;
- C. A description of each type of information that was affected by the Covered Incident;
- D. The number of consumers whose information was affected by the Covered Incident;
- E. The acts that each Covered Business has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of each materially different notice sent by each Covered Business to consumers or to any U.S. federal, state, or local government entity regarding the Covered Incident.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed 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 begin, “*In re Rite Aid Corporation*, FTC File No. C-4308.”

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 members; (2) all of Respondents’ current and future subsidiaries that own, control, 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 Respondent; (b) identify all of that Respondent’s businesses by all of 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

structure of such Respondent or any entity that such Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order;

- C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within fourteen (14) days of its filing;
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature;
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed 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 begin: “In re Rite Aid Corporation, FTC File No. C-4308”.

XV. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years, unless otherwise specified below. Specifically, Respondents must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints concerning the subject matter of this Order, whether received directly or indirectly, such as through a third party, and any response;
- D. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission;
- E. For five (5) years after the date of preparation of each System Assessment required by this Order, all materials relied upon to prepare the System Assessment, including all

plans, test results, reports, studies, reviews, audits, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related 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 any representation concerning a change in any website or other service controlled by Respondents that relates to privacy, security, availability, confidentiality, or integrity of Covered Information;
- G. For five (5) years after the date of preparation of each Assessment by the Assessor, as those terms are defined in Provision IX, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning compliance with related Provisions of this Order, for the compliance period covered by such Assessment;
- H. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondents' compliance with this Order; and
- I. For five (5) years from the date created or received, all records, whether prepared by or on behalf of a Respondent, that tend to show any lack of compliance by a Respondent with this Order.

XVI. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its

representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVII. Modification of Original Decision and Order

IT IS FURTHER ORDERED that this Decision and Order supersedes the Decision and Order the Commission previously issued in *In re Rite Aid Corporation*, C-4308, 150 F.T.C. 694 (Nov. 12, 2010).

XVIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision 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 Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the 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 Provision 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.

April Tabor
Secretary

SEAL:
ISSUED: