

Complaint

IN THE MATTER OF

AARON’S, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4442; File No. 122 3264
Complaint, March 10, 2014 – Decision, March 10, 2014

This consent order addresses Aaron’s, Inc.’s use of PC Rental Agent, a privacy-invasive software that many of its franchisees installed on computers rented to consumers. The complaint alleges that Aaron’s knowingly assisted its franchisees by allowing them to access DesignerWare’s website, which was necessary in order for them to use PC Rental Agent to activate Detective Mode and secretly monitored consumers’ activities on rented computers. Second, Aaron’s corporate server was used to transmit and store a voluminous number of emails containing Detective Mode content. The complaint further alleges that Aaron’s knew the data being gathered by Detective Mode could be highly intrusive and invaded consumers’ privacy; and that, as a result of Aaron’s practices, consumers were substantially harmed. The consent order requires the destruction of any data using monitoring or tracking technology without the requisite notice and consent or obtained under false pretenses, and mandates the encryption of any properly collected data when it is transmitted. The order also requires Aaron’s to oversee and monitor its franchisees to ensure that their conduct complies with the core constraints imposed on Aaron’s, which prohibits the deceptive gathering of consumer information such as using fake software registration notices or similar deceptive tactics.

Participants

For the *Commission*: Julie K. Mayer and Tracy S. Thorleifson.

For the *Respondent*: Kristy Brown and Jim Harvey, Alston & Bird LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Aaron’s, Inc., has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Aaron’s, Inc., (“Aaron’s” or “respondent”), is a Georgia corporation with its principal office or place of business at 309 E. Paces Ferry Road, N.E., Atlanta, Georgia 30305.

Complaint

Aaron's is a national "rent-to-own" ("RTO") retailer of consumer electronics, residential furniture, and household appliances. RTO retailers allow consumers to rent goods with an option to purchase them.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Aaron's does business through a network of more than 1,300 company-owned stores and 700 independently owned franchised stores that operate across the United States. Since at least 2009 through January 2012, some Aaron's franchisees licensed a software product known as PC Rental Agent from DesignerWare, LLC ("DesignerWare") and installed it on computers rented to consumers. Aaron's knew that some of its franchisees had installed PC Rental Agent on computers rented to consumers because, among other things, Aaron's provided these stores with the technical capacity to access and use PC Rental Agent, as detailed below. Company-owned Aaron's stores did not license or use PC Rental Agent.

4. When installed on a rented computer, PC Rental Agent enabled Aaron's franchisees to disable a computer remotely. PC Rental Agent also enabled Aaron's franchisees to remotely install and activate an add-on program called Detective Mode. Using Detective Mode, Aaron's franchisees could – and did – surreptitiously monitor the activities of computer users, including by logging keystrokes, capturing screenshots, and using the computer's webcam. Through Detective Mode, Aaron's franchisees could – and did – secretly gather consumers' personal information using fake software registration windows. In addition, using a different PC Rental Agent feature, Aaron's franchisees tracked the physical location of rented computers using WiFi hotspot location information. Aaron's franchisees used this illicitly gathered data to assist in collecting past-due payments and recovering computers after default.

Complaint

5. Detective Mode data sent to Aaron's franchisees revealed private, confidential, and personal details about consumers using rented computers. Keystroke logs displayed usernames and passwords for access to email accounts, social media websites, and financial institutions. Screenshots captured additional confidential details, including medical information, applications containing Social Security numbers, and bank and credit card statements. Webcams operating secretly inside computer users' homes took photographs of computer users and anyone else within view of the camera. These included images of minor children as well as individuals not fully clothed and engaged in intimate conduct. The presence of PC Rental Agent was not detectable to computer users and computer renters could not uninstall it. In numerous instances, Aaron's franchisees did not obtain consent from their rental customers and did not disclose to them or the rental computers' users that PC Rental Agent was installed and could be used to track consumers' physical locations and remotely spy on their activities.

6. To use PC Rental Agent and activate Detective Mode, Aaron's franchisees needed to access DesignerWare's website and direct PC Rental Agent to take the desired action. Aaron's franchisees also needed to provide DesignerWare with an email address to which DesignerWare could send data captured by Detective Mode. DesignerWare forwarded immediately all data collected by Detective Mode to the email address provided by the Aaron's franchisee. Because at one activation level Detective Mode would capture screen shots, log keystrokes, and take webcam pictures every two minutes that the computer was connected to the Internet until directed to stop, and because this data was contemporaneously emailed to the Aaron's franchisees requesting it, Detective Mode activations often generated an enormous volume of data.

7. Aaron's requires its franchisees to have company-provided, Aarons.com email addresses. Aaron's also provides these franchisees with email accounts and server space to store email messages. Such email messages are routed through Aaron's corporate headquarters and stored on computer servers owned, controlled, and maintained by Aaron's. Under the franchise agreement that governs each Aaron's franchisee, Aaron's may terminate a franchisee that breaches any Aaron's policy or

Complaint

practice or that violates federal, state, or local laws, regulations, or ordinances. In addition, Aaron's policies and training materials for franchisees prohibit "unlawful" computer and Internet use, and set standards for fair collection practices.

8. Aaron's protects its computer network with certain security features. DesignerWare's website, through which Aaron's franchisees needed to access PC Rental Agent and activate Detective Mode, did not interface smoothly with Aaron's network configurations. In numerous instances, Aaron's franchisees had to seek written permission from Aaron's to access the DesignerWare website so that they could use PC Rental Agent. Senior Aaron's management approved these requests and authorized franchisees to access the DesignerWare website using the Aaron's network. Absent this permission, many Aaron's franchisees could not have used PC Rental Agent, activated Detective Mode, and surreptitiously monitored consumers' activities on rented computers.

9. Aaron's also provided its franchisees with troubleshooting advice relating to installation of PC Rental Agent software on rental computers. Technical conflicts between PC Rental Agent and the antivirus program already installed on computers in rental inventory prevented franchisees from readily installing PC Rental Agent. Aaron's published step-by-step instructions for installing PC Rental Agent on Aaron's rental computers in a newsletter for franchisees and posted those instructions on its website.

10. In numerous instances, Aaron's franchisees used the Aaron's computer network to access the DesignerWare website, and then, often using instructions provided by Aaron's, installed PC Rental Agent on computers rented to consumers. Aaron's franchisees directed DesignerWare to send Detective Mode data to the email accounts provided to them by Aaron's. Aaron's computer network was used to receive, store, and access upwards of 100,000 Detective Mode messages, including messages containing private and confidential consumer information about consumers who rented computers from Aaron's franchisees. Aaron's has stored such messages on its computer network since at least 2009.

Complaint

11. Aaron's knew that Detective Mode captured confidential and personal information from consumer computer users without notice to those users. Aaron's IT personnel were aware that company server space was being used to store Detective Mode emails and knew what data those emails contained. One IT employee who reviewed Detective Mode images sent to a franchisee described the program as "very intrusive" in an email to Aaron's chief information officer.

12. Aaron's employees responsible for franchisee development and oversight, "franchise representatives," also knew that Aaron's franchisees were installing PC Rental Agent and using Detective Mode without notice to consumers. Franchise representatives discussed PC Rental Agent with franchisee employees, via email and in-person, including at Aaron's-sponsored conferences attended by franchisee employees where PC Rental Agent was an agenda item. Some franchisee employees first heard about PC Rental Agent from Aaron's franchise representatives. Through these communications, Aaron's employees also learned about the privacy-invasive capabilities of Detective Mode. For example, one franchisee owner suggested to an Aaron's franchise representative that PC Rental Agent use be put on the agenda for an upcoming meeting in part because he said he was "a little uncomfortable with the ability to see the customer through the webcam."

13. Beginning at least in 2010 and throughout 2011, Aaron's senior corporate management not only knew that its franchisees were using PC Rental Agent and activating Detective Mode without notice to computer users, they also knew that data and information gathered by Detective Mode could be highly intrusive and invaded consumers' privacy. Aaron's managers specifically discussed whether to purchase PC Rental Agent for installation on Aaron's corporate-owned stores. As part of that discussion, Aaron's reviewed the use of PC Rental Agent by some of its franchisees, as well as Detective Mode's capabilities. Among other things, managers received email communications that included examples of images captured by Detective Mode. Ultimately, Aaron's decided not to purchase PC Rental Agent for its corporate stores.

Complaint

14. Aaron's management learned even more about PC Rental Agent and Detective Mode when, in May 2011, Aaron's was sued by a franchisee customer who alleged that an Aaron's franchisee's use of Detective Mode invaded her privacy and violated state and federal law. The lawsuit, which also named the Aaron's franchisee and DesignerWare, was styled as a class action. The complaint described, *inter alia*, the alleged properties of Detective Mode, including its capacity to capture computer users' keystrokes, screenshots of their computer activities, and webcam images.

15. Aaron's did not close its web portal and revoke franchisee access to the DesignerWare website and Detective Mode emails until December 2011. Following that action by Aaron's, its franchisees that used Aaron's network could no longer receive and view emails from DesignerWare containing Detective Mode-captured data about their customers. Aaron's computer servers received the last Detective Mode email in January 2012. Aaron's failed to act earlier despite clear authority to control its franchisees' access to and use of Aaron's computer network.

16. Aaron's conduct in permitting and participating in the gathering and storage of private and confidential information about individuals caused or was likely to cause substantial harm to consumers. Because of Aaron's actions, private and confidential information was captured, stored on Aaron's computer system, and revealed to Aaron's franchisees. This conduct placed consumers at risk from the exposure of their personal, financial account access, and medical information. Consumers also were injured by the unwarranted invasion into the peaceful enjoyment of their homes. Detective Mode's surreptitious capture of the private details of individual and family life – including images of visitors, children, family interactions, partially undressed individuals, and people engaged in intimate conduct – caused actual consumer harm. Because Detective Mode functioned secretly, consumers were unable to reasonably avoid this harm, which was neither trivial nor speculative. Further, the harm caused by the knowing and unauthorized gathering and storage of private and confidential information is not outweighed by countervailing benefits to consumers or to competition.

Decision and Order

VIOLATION OF THE FTC ACT

17. Through the means described in Paragraphs 3 through 16, respondent's actions have caused or are likely to cause substantial injury to consumers that cannot be reasonably avoided and is not outweighed by countervailing benefits to consumers or competition. Therefore, respondent's practices constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission, this tenth day of March, 2014, has issued this complaint against respondent.

By the Commission.

DECISION AND ORDER

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

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the respondent

Decision and Order

has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such consent agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent Aaron, Inc. ("Aaron's"), is a Georgia corporation with its principal office or place of business at 309 E. Paces Ferry Road, N.E., Atlanta, Georgia 30305.
2. The Commission has jurisdiction of the subject matter of this proceeding and of respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

- A. Unless otherwise specified, "respondent" shall mean Aaron's and its successors and assigns.
- B. "Commerce" shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
- C. "Computer" shall mean any desktop or laptop computer, handheld device, tablet, smartphone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content.

Decision and Order

D. “Clear(ly) and prominent(ly)” shall mean:

1. In textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
2. In communications disseminated orally or through audible means (e.g., radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
3. In communications disseminated through video means (e.g., television or streaming video), the required disclosures are in writing in a form consistent with subpart (a) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication;
4. In communications made through interactive media, such as the Internet, online services, and software, the required disclosures are unavoidable and presented in a form consistent with subpart (a) of this definition, in addition to any audio or video presentation of them; and
5. In all instances, the required disclosures are presented in an understandable language and syntax; in the same language as the predominant language that is used in the communication; and include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

Decision and Order

- E. “Consumer product” shall mean any item that is primarily for personal, family, or household use.
- F. “Covered rent-to-own transaction” shall mean any transaction where a consumer enters into an agreement for the purchase or rental of any consumer product where the consumer’s contract or rental agreement provides for payments over time with options to purchase the product.
- G. “Franchisee” shall mean an independently owned business that operates under a franchise agreement with respondent.
- H. “Geophysical location tracking technology” shall mean any hardware, software, or application that collects and reports data or information that identifies the precise geophysical location of an item. Geophysical location tracking technologies include, but are not limited to, technologies that report the GPS coordinates of a computer or other item; the WiFi signals available to or actually used by a computer to access the Internet; the telecommunication towers or connections available to or actually used by a computer; the processing of any such reported data or information through geolocation lookup services; or any information derived from any combination of the foregoing.
- I. “Monitoring technology” shall mean any hardware, software, or application utilized in conjunction with a computer that can cause the computer to (1) capture, monitor, or record, and (2) report information about user activities by:
 - 1. Recording keystrokes, clicks, or other user-generated actions;
 - 2. Capturing screenshots of the information displayed on a computer monitor or screen; or
 - 3. Activating the camera or microphone function of a computer to take photographs or record audio or

Decision and Order

visual content through the computer's webcam or microphone.

INJUNCTION**I.****MONITORING TECHNOLOGY PROHIBITED**

IT IS HEREBY ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with them who receive actual notice of this order, by personal service or otherwise, in connection with any covered rent-to-own transaction, are hereby permanently restrained and enjoined from:

- A. Using any monitoring technology to gather data or information from or about a consumer from any computer rented to a consumer; or
- B. Receiving, storing, or communicating any data or information from or about a consumer that was gathered from a computer rented to a consumer using any monitoring technology.

Provided that this Part does not apply to respondent's use of any monitoring technology to gather data or information from or about a consumer from any computer rented to a consumer, with notice to and consent from the consumer, in connection with a request for technical assistance initiated by the consumer, where respondent only uses the information to provide, or attempt to provide, the requested technical assistance and for no other purpose.

II.**USE OF TRACKING TECHNOLOGY LIMITED**

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with them who receive actual notice of this Order, by

Decision and Order

personal service or otherwise, in connection with any covered rent-to-own transaction, are hereby permanently restrained and enjoined from:

- A. Gathering any data or information from any consumer product via any geophysical location tracking technology without providing clear and prominent notice to the consumer who rented the product at the time it is rented and also obtaining affirmative express consent from the consumer at the time the consumer product is rented;
- B. Failing to provide clear and prominent notice to consumers and obtaining affirmative express consent from consumers at the time any consumer product is rented, to the extent that such notice and consent are required by subpart A, above, by the following means:
 - 1. Clear and Prominent Notice: respondent shall provide a clear and prominent notice to the user, separate and apart from any “privacy policy,” “data use policy,” “terms of service,” “end-user license agreement,” “lease agreement,” or other similar document, that discloses (1) that geophysical location tracking technology is installed and/or currently running on the rented consumer product; (2) the types of user activity or conduct that is being captured by such technology; (3) the identities or specific categories of entities with whom any data or information that is collected will be shared or otherwise provided; (4) the purpose(s) for the collection, use, or sharing of such data or information; and (5) where and how the consumer can contact someone for additional information; and
 - 2. Affirmative Express Consent: respondent shall obtain affirmative express consent by giving the renter an equally clear and prominent choice to either agree or not agree to any geophysical location tracking technology, and neither option may be highlighted or preselected as a default

Decision and Order

setting. Activation of any geophysical location tracking technology must not proceed until the renter provides affirmative express consent. Notwithstanding the foregoing, nothing in this Section shall require respondent to rent an item to a consumer who declines to consent to installation or activation of any geophysical tracking technology; and

- C. In connection with the rental of computers, installing or activating on rented computers geophysical location tracking technology where that technology does not provide clear and prominent notice to the computer user immediately prior to each use of the geophysical location tracking technology, as clear and prominent is defined above, and by the installation of a clear and prominent icon on the computer on which the technology is installed, such as on the desktop and in the desktop system tray of the computer. Clicking on the icon must clearly and prominently disclose: (1) that geophysical location tracking technology is installed and currently running on the computer; (2) the types of user activity or conduct that is being captured by such technology; (3) the identities or specific categories of entities with whom any data or information that is collected will be shared or otherwise provided; (4) the purpose(s) for the collection, use, or sharing of such data or information; and (5) where and how the user can contact someone for additional information.

Provided that respondent may suspend the notice requirements of this Part and activate geophysical location tracking technology if a) the consumer reports that a rented consumer product has been stolen or respondent otherwise has a reasonable basis to believe that a rented consumer product has been stolen, and b) either the consumer or respondent has filed a police report stating that the consumer product has been stolen. Provided further that respondent shall retain documents establishing (a) and (b). For purposes of this Order, “filing of a police report” means the filing of the consumer’s or respondent’s complaint with the police department in any form recognized in the jurisdiction.

Decision and Order

Provided further that this Part does not apply to respondent's use of geophysical location tracking technology, with notice to and consent from a consumer to the extent that such notice and consent are required by subpart A, to gather data or information in connection with a request for technical assistance initiated by a consumer, where respondent only uses the information to provide, or attempt to provide, the requested technical assistance and for no other purpose.

III.**NO DECEPTIVE GATHERING OF CONSUMER INFORMATION**

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with them who receive actual notice of this Order, by personal service or otherwise, in connection with any covered rent-to-own transaction, are hereby permanently restrained and enjoined from making or causing to be made, or assisting others in making or causing to be made, any false representation or depiction in any notice, prompt screen, or other software application appearing on the screen of any computer that results in gathering data or information from or about a consumer.

IV.**NO USE OF IMPROPERLY OBTAINED INFORMATION IN COLLECTIONS**

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with them who receive actual notice of this Order, by personal service or otherwise, are hereby permanently restrained and enjoined from using, in connection with collecting or attempting to collect a debt, money, or property pursuant to a covered rent-to-own transaction, any data or information from or about a consumer obtained in a manner that does not comply with Parts I, II, and III of this Order.

Decision and Order

**V.
PROTECTION OF DATA**

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with them who receive actual notice of this Order, by personal service or otherwise, shall:

- A. Delete or destroy data or information from or about a consumer previously gathered or stored using any monitoring or geophysical location tracking technology that does not comply with Parts I, II, and III of this Order, unless such action is otherwise prohibited by court order or other legal obligation and after the expiration of any such court order or other legal obligation the information is deleted or destroyed; and
- B. Only transfer any data or information from or about a consumer that was gathered by any monitoring or geophysical location tracking technology from the computer upon which the technology is installed to respondent's server(s), and from the respondent's server(s) to any other computers or servers, if the information collected is rendered unreadable, unusable, or indecipherable during transmission.

**VI.
NO MISREPRESENTATIONS ABOUT PRIVACY**

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, and its officers, agents, servants, employees, and all persons or entities in active concert or participation with it who receive actual notice of this Order, by personal service or otherwise, in connection with any covered rent-to-own transaction shall not misrepresent, in any manner, expressly or by implication, the extent to which respondent maintains and protects the security, privacy, or confidentiality of any data or information from or about a consumer.

Decision and Order

VII.
OVERSIGHT AND MONITORING OF FRANCHISEES

IT IS FURTHER ORDERED that respondent shall:

- A. Require its franchisees to delete or destroy data or information from or about a consumer previously gathered or stored using any monitoring or geophysical location tracking technology that does not comply with Parts I, II, and III of this Order, unless such action is otherwise prohibited by court order or other legal obligation, in which case, after the expiration of any such court order or other legal obligation, respondent shall require its franchisees to delete or destroy the data or information;
- B. Within thirty (30) days after the date of service of this Order, prohibit each of its franchisees from, in connection with a covered rent-to-own transaction:
 - 1. Using any monitoring technology to gather data or information from or about a consumer from any computer rented to a consumer;
 - 2. Receiving, storing, or communicating any data or information from or about a consumer that was gathered from a computer rented to a consumer using any monitoring technology;
 - 3. Gathering any data or information from any consumer product via any geophysical location tracking technology in a manner that:
 - a. does not comply with Part II of this Order; and
 - b. that respondent has not approved in advance of the franchisee's use of such technology;
 - 4. Using, in connection with collecting or attempting to collect a debt, money, or property pursuant to a covered rent-to-own transaction, any data or information from or about a consumer obtained in

Decision and Order

a manner that does not comply with Parts I, II, and III of this Order; and

5. Making, or causing to be made, any false representation or depiction in any notice, prompt screen, or other software application appearing on the screen of any computer that results in gathering data or information from or about a consumer;
- C. Monitor compliance by each franchisee with the requirements of Parts VII.A and VII.B, including but not limited to by annually reviewing each franchisee's compliance with Parts VII.A. and VII.B.; and
- D. When respondent knows, or has reason to know, whether as a result of monitoring required by Part VII.C. or otherwise, that a franchisee has violated any requirement imposed on that franchisee by respondent in compliance with Parts VII.A. or VII.B.:
1. Immediately take action to ensure that the franchisee corrects its practices; and
 2. Terminate any such franchisee that fails to make such correction.

VIII.
DISTRIBUTION OF ORDER

IT IS FURTHER ORDERED that respondent must deliver a copy of this Order to all current and future principals, officers, directors, and managers who have responsibilities related to the subject matter of this Order and to all franchisee principals. Delivery must occur within thirty (30) days after the date of service of the Order for current personnel and franchisee principals. For new personnel and franchisee principals, delivery must occur before they assume their responsibilities. From each individual to whom respondent delivers a copy of this Order, respondent must obtain a signed and dated acknowledgment of receipt of this Order, with any electronic signatures complying with the requirements of the E-Sign Act, 15 U.S.C. § 7001 et seq.

Decision and Order

IX.
COMPLIANCE REPORTING

IT IS FURTHER ORDERED that:

- A. Respondent, and its successors and assigns, shall, within sixty (60) days after the date of service of this Order, and at such other times as the Commission may require, file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which they have complied with this Order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports;
- B. Respondent, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this Order, including, but not limited to, dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or related entity that engages in any acts or practices subject to this Order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, the respondent shall notify the Commission as soon as is practicable after obtaining such knowledge; and
- C. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, with the subject line *In re Aaron's, Inc.*, File No. 1223264. *Provided, however*, that, in lieu of overnight courier, notices may be sent by first class mail, but

Decision and Order

only if an electronic version of each such notice is contemporaneously sent to the Commission at DEbrief@ftc.gov.

**X.
RECORDKEEPING**

IT IS FURTHER ORDERED that respondent shall, for five (5) years after the last date of any act or practice covered by Parts I – VII of this Order, maintain and upon reasonable notice make available to the Federal Trade Commission for inspection and copying, any documents, whether prepared by or on behalf of respondent, that:

- A. Comprise or relate to complaints or inquiries, whether received directly, indirectly, or through any third party, concerning consumer privacy, specifically including complaints or inquiries related to any monitoring or geophysical tracking technologies and any responses to those complaints or inquiries;
- B. Are reasonably necessary to demonstrate full compliance with each provision of this Order, including but not limited to, all documents obtained, created, generated, or which in any way relate to the requirements, provisions, or terms of this Order, and all reports submitted to the Commission pursuant to this Order;
- C. Contradict, qualify, or call into question respondent's compliance with this Order; or
- D. Acknowledge receipt of this Order obtained pursuant to Part VIII.

**XI.
TERMINATION OF ORDER**

This Order will terminate on March 10, 2034, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any

Analysis to Aid Public Comment

violation of the Order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this Order that terminates in less than twenty (20) years; and
- B. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

Provided, further, that, if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Part as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Aaron's, Inc.

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

The Commission's administrative complaint alleges that respondent Aaron's engaged in unfair practices that caused, or are

Analysis to Aid Public Comment

likely to cause, substantial injury to consumers that cannot be reasonably avoided and are not outweighed by countervailing benefits to consumers or competition.

Aaron's, an operator and franchisor of more than 1,300 corporate and nearly 750 franchisee rent-to-own ("RTO") stores across the country and Canada, played an important role in the use of PC Rental Agent, a privacy-invasive software that many of its franchisees installed on computers rented to consumers. PC Rental Agent surreptitiously collected private, confidential, and personal information about consumers who used rented computers. RTO stores that licensed PC Rental Agent from its manufacturer, DesignerWare, could use this illicitly gathered data about their customers to assist in collecting on past-due accounts and recovering computers after default. When in its "Detective Mode," PC Rental Agent could log keystrokes, capture screenshots, and activate a computer's webcam. Detective Mode also allowed users to deceptively gather consumers' personal information through fake software registration notices. Information that Detective Mode collected was transmitted from rented computers to DesignerWare, which in turn would email it to its licensees, including Aaron's franchisees. Another feature of PC Rental Agent allowed RTO stores to track the physical location of rented computers using WiFi hotspot information, which RTO store licensees could access by logging onto DesignerWare's website.

According to the Commission's complaint, Aaron's knowingly assisted its franchisees in using PC Rental Agent in a variety of ways. First, Aaron's specifically allowed its franchisees to access DesignerWare's website, which was necessary in order for them to use PC Rental Agent. Without this permission from Aaron's, many of its franchisees could not have activated Detective Mode and secretly monitored consumers' activities on rented computers. Second, Aaron's corporate server was used to transmit and store a voluminous number of emails containing Detective Mode content. Aaron's provided email accounts to its franchisees that many of them used to receive messages sent from DesignerWare containing Detective Mode-captured information. Emails sent to and from these accounts were routed through Aaron's corporate headquarters and stored on computer servers owned, controlled, and maintained by Aaron's.

Analysis to Aid Public Comment

As a result, Aaron's maintained on its corporate server upwards of 100,000 Detective Mode messages containing covertly gathered consumer information. Finally, Aaron's provided franchisees with vital technical support about PC Rental Agent. For example, Aaron's published trouble-shooting advice about installing the program on rented computers and avoiding conflicts with antivirus software.

The proposed complaint alleges that, as a result of Aaron's practices, consumers were substantially harmed. It further alleges that Aaron's knew the data being gathered by Detective Mode could be highly intrusive and invaded consumers' privacy. This knowing support of franchisees' use of Detective Mode without notice to computer users placed those consumers at risk from exposure of their personal, financial account access, and medical information. Consumers were also injured by the unwarranted invasion into the peaceful enjoyment of their homes. Detective Mode's surreptitious capture of the private details of individual and family life – including images of visitors, children, family interactions, partially undressed individuals, and people engaged in intimate conduct – caused actual consumer harm. Because Detective Mode functioned secretly, consumers were unable to reasonably avoid this harm, which was neither trivial nor speculative. Further, there were no countervailing benefits to consumers or to Aaron's that outweighed this harm.

The proposed consent order contains provisions designed to prevent Aaron's and its franchisees from engaging in the challenged practices and similar future conduct. Section I of the order prohibits Aaron's from using monitoring technology on computers and from receiving, storing, or communicating information about consumers collected with such technology. Section II prohibits Aaron's use of geophysical location tracking technology on any consumer product without notifying and obtaining consent from renters. Aaron's must also notify a user of a rented computer immediately prior to activating tracking technology on that device, unless Aaron's has a reasonable basis to believe that the computer has been stolen and a police report filed. Both Sections I and II also contain provisos that permit Aaron's to use monitoring or geophysical location tracking technology for purposes of providing requested customer assistance, where the consumer has consented to the use of the

Analysis to Aid Public Comment

technology and any information collected is used only to provide the requested assistance.

Section III of the proposed order prohibits the deceptive gathering of consumer information, which will bar Aaron's from using fake software registration notices or similar deceptive tactics. Section IV will prevent Aaron's from using any consumer information to collect on rental contracts that was improperly obtained through monitoring technology, tracking technology, or deceptive notices that appear on computer screens. Section V requires the destruction of any data using monitoring or tracking technology without the requisite notice and consent or obtained under false pretenses, and mandates the encryption of any properly collected data when it is transmitted. Section VI prohibits Aaron's from making any misrepresentations about the privacy or security of consumer information it collects.

The order also contains provisions that require Aaron's to oversee and monitor its franchisees to ensure that their conduct complies with the core constraints imposed on Aaron's. Section VII mandates that Aaron's require its franchisees to delete or destroy any consumer information improperly gathered via monitoring technology, tracking technology, or deceptive notices that appear on computer screens. Under that section, Aaron's must also prohibit its franchisees from: 1) using any monitoring technology to gather consumer information from a leased computer; 2) receiving, storing, or communicating any data gathered using monitoring technology; 3) using any geophysical location tracking technology that Aaron's has not approved in advance; 4) gathering any data from any consumer product using geophysical location tracking technology without providing notice and consent; 5) using any improperly gathered consumer information to collect a debt; and 6) making a false representation to a consumer through the use of fake software registration notices or other deceptive statements that appear on the screen of a computer. Aaron's must also monitor, on an annual basis or more frequently, its franchisees' compliance with these requirements and, if Aaron's learns through this process or otherwise has reason to know that a franchisee has violated Section VII of the order, it must take immediate action to ensure that the franchisee corrects its practices. If it does not, Aaron's must terminate that franchisee.

Analysis to Aid Public Comment

Sections VIII – XI of the proposed order contain order distribution, compliance reporting, and recordkeeping provisions. Section VIII requires Aaron's to disseminate the order to persons with responsibilities related to the subject matter of the order, including franchisee principals. It also requires Aaron's to secure a signed and dated statement acknowledging receipt of the order from all persons who receive a copy. Section IX imposes standard reporting requirements, requiring Aaron's to file compliance reports to the Commission within sixty (60) days and periodically thereafter upon request. This section also requires that Aaron's notify the Commission of any changes in corporate status. Section X mandates that, for five (5) years, Aaron's retain documents relating to its compliance with the order and about complaints or inquiries concerning consumer privacy. Finally, Section XI is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

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

Complaint

IN THE MATTER OF

DOWN TO EARTH DESIGNS, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4443; File No. 122 3268
Complaint, March 18, 2014 – Decision, March 18, 2014

This consent order addresses Down to Earth Designs, Inc. d/b/a gDiapers' marketing, sale, and distribution of diapers and baby wipes with claims of various environmental benefits. The complaint alleges that respondent represented that its diapers and wipes are biodegradable, "certified 100% biodegradable," garbage free when trashed or flushed, and plastic free. The complaint further alleges that respondent failed to disclose adequately that consumers can safely compost only wet used inserts and wipes. The consent order requires respondent to clearly and prominently disclose the time to complete decomposition or the rate and extent of decomposition with a further disclosure that the stated rate and extent of decomposition does not mean that the item will continue to decompose, if the item does not completely decompose within one year after customary disposal. The order also prohibits respondent from making specific environmental claims about any product or package unless the claim is true, not misleading, and substantiated by competent and reliable scientific evidence.

Participants

For the *Commission*: Matthew Wilshire and Boris Yankilovich.

For the *Respondent*: Ann M. Begley and Zachary A. Rothstein,
Morgan, Lewis & Bockius LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Down to Earth Designs, Inc., d/b/a gDiapers ("Respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent is an Oregon corporation with its principal place of business at 2808 NE Martin Luther King Jr. Boulevard, Portland, Oregon, 97212.