

Complaint

IN THE MATTER OF

DESIGNERWARE, LLCCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4390; File No. 112 3151
Complaint, April 11, 2013 – Decision, April 11, 2013

This consent order addresses allegations that DesignerWare, LLC's PC Rental Agent software program violated consumers' privacy by collecting confidential information without consumers' knowledge or consent. DesignerWare developed the PC Rental Agent software to aid rent-to-own stores in tracking and recovering rented computers; to render computers inoperable if consumers are late or default on payments or are stolen; and to erase computer hard drives for redistribution. The software featured an add-on program called "Detective Mode" that purported to locate rented computers. The complaint alleges that Designerware intentionally used the PC Rental Agent software and the Detective Mode add-on program to spy on consumers by logging each user's keystrokes; capturing screenshots; taking pictures with the computer's webcam; gathering confidential personal, financial, and medical data; and sending this data to DesignerWare's servers. The consent order prohibits DesignerWare from gathering and disclosing consumers' personal information collected during Detective Mode and from using geophysical location tracking technology without consumer consent. The order further imposes compliance reporting and notification requirements.

Participants

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

For the *Respondent*: Robert Bernstein, Bernstein Law Firm.

COMPLAINT

The Federal Trade Commission, having reason to believe that DesignerWare, LLC, a corporation, and Timothy Kelly and Ronald P. Koller, individually and as officers of the corporation ("respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

Complaint

1. Respondent DesignerWare, LLC (“DesignerWare”), is a Nevada limited liability corporation with its principal office or place of business at 108 Hutchinson Drive, North East, Pennsylvania 16428.

2. Respondent Timothy Kelly is an officer and owner of DesignerWare. Individually or in concert with others, he formulates, directs, or controls the policies, acts, or practices of DesignerWare, including the acts or practices alleged in this complaint. His principal office or place of business is 108 Hutchinson Drive, North East, Pennsylvania 16428.

3. Respondent Ronald P. Koller was an officer and owner of DesignerWare until on or about March 28, 2012. Individually or in concert with others, at all relevant times, he formulated, directed, or controlled the policies, acts, or practices of DesignerWare, including the acts or practices alleged in this complaint. He resides in Ocoee, Florida.

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

RESPONDENTS’ BUSINESS PRACTICES

5. Respondents developed a software product called PC Rental Agent that they license to stores in the rent-to-own industry. Rent-to-own stores allow consumers to rent, with an option to purchase, goods such as furniture, household appliances, and consumer electronics including computers. Typically, the rental agreement will include an option for the consumer to purchase the rented item for a fixed sum after making a certain number of payments. PC Rental Agent, when installed on a rented computer, offers rent-to-own store licensees the ability to direct DesignerWare’s servers to disable a computer remotely when a consumer is late making payments, has stopped communicating with the rent-to-own store, or has otherwise violated the rental contract. As of August 2011, approximately 1,617 rent-to-own stores in the United States, Canada, and Australia have licensed PC Rental Agent. PC Rental Agent has been installed on approximately 420,000 computers worldwide.

Complaint

6. Through PC Rental Agent, DesignerWare offers rent-to-own store licensees additional functions and features, including the ability to direct DesignerWare's servers to track and report the physical location of a computer and to activate an add-on program called Detective Mode that enables licensees to monitor surreptitiously the activities of the computer's user, including by using the computer's webcam. Through Detective Mode, rent-to-own store licensees can also direct DesignerWare's servers to cause fake software registration windows to pop-up on rented computers and gather consumer's personal information.

7. Rent-to-own stores typically install PC Rental Agent on computers rented to consumers prior to the consumer taking possession of the computer. The presence of PC Rental Agent is not detectable to a computer's user and the computer's renter cannot uninstall it.

8. DesignerWare recommends, but does not require, contractually or otherwise, that its licensees disclose the presence of PC Rental Agent on a rented computer at the time the consumer signs the initial rental contract. DesignerWare takes no steps to determine whether its licensees follow its recommendation and disclose the presence of PC Rental Agent to computer renters. In numerous instances, rent-to-own stores do not disclose to consumers that they have installed and/or are using PC Rental Agent on rented computers. DesignerWare designed the Detective Mode program to operate without the computer user's knowledge, and advises rent-to-own store licensees to install and activate Detective Mode without notice to the computer user.

9. To administer PC Rental Agent commands, rent-to-own store licensees must log on to DesignerWare's website and direct PC Rental Agent to take the desired action on a particular computer. DesignerWare receives reports from computers on which PC Rental Agent is installed every two hours while the computer is connected to the Internet. When a computer reports to DesignerWare, PC Rental Agent executes any commands it has received from a licensee, including, for example, a command to activate Detective Mode.

Complaint

Monitoring Computer Users via Detective Mode

10. Since at least 2007, DesignerWare has made available to PC Rental Agent licensees an add-on program, Detective Mode. Through DesignerWare, rent-to-own stores can cause Detective Mode to be installed and activated on any computer with PC Rental Agent without telling the computer's renter. DesignerWare limits access to the Detective Mode function to one "Master Account Holder" designated by the licensee. DesignerWare does not charge licensees extra for the use of Detective Mode, nor does DesignerWare sell the program separately from PC Rental Agent.

11. Once installed and activated, Detective Mode can log the keystrokes of the computer user, take screen shots of the computer user's activities on the computer, and photograph anyone within view of the computer's webcam. Detective Mode secretly gathers this information and transmits it to DesignerWare, who then transmits it to the rent-to-own store from which the computer was rented, unbeknownst to the individual using the computer.

12. Respondent Tim Kelly described PC Rental Agent this way in an August 26, 2010 email:

The way the Detective [Detective Mode] works is like many spyware/malware programs. The Agent [PC Rental Agent] runs outside the user session so it is not detectable by antivirus programs, etc. However when you turn on the Detective, the Agent takes an executable and inject[s] it into the user session and hooks the screen, keyboard, and mouse so it can 'Spy' on the user and gather information. A similar program could be launched to steal credit cards or someone's information.

13. DesignerWare recommends that its licensees install and activate Detective Mode only to locate and identify the person in possession of a lost or stolen computer. It asserts that a consumer who is late in making lease payments has "stolen" the computer. DesignerWare does not monitor its own collection of, or limit its licensees' access to, Detective Mode data to ensure that the information was obtained and used only for designated purposes. In numerous instances, rent-to-own store licensees have caused

Complaint

Detective Mode to be installed and activated on computers where consumers were late in making rental payments and where the licensees had no reason to believe the computers had been the subject of criminal theft.

14. Detective Mode gathers data about whoever is using the computer, whether it is the computer's renter or another individual. At one level of activation, Detective Mode will gather data and transmit it to DesignerWare every two minutes that the computer is connected to the Internet for a period of 60 minutes. DesignerWare then forwards the data to the licensee who activated "the Detective." If the rent-to-own store wants more information, it can cause Detective Mode to record data every two minutes until prompted to stop doing so. DesignerWare's servers collect this information and transmit it to the licensee for however long the licensee leaves "the Detective" turned on. In numerous instances, data gathered by Detective Mode has revealed private, confidential, and personal details about the computer user. For example, keystroke logs have displayed usernames and passwords for access to email accounts, social media websites, and financial institutions. Screenshots have captured additional confidential and personal information, including medical records, private emails to doctors, employment applications containing Social Security numbers, bank and credit card statements, and discussions of defense strategies in a pending lawsuit. When activated, Detective Mode can also cause a computer's webcam to surreptitiously photograph not only the computer user, but also anyone else within view of the camera. In numerous instances, Detective Mode webcam activations have taken pictures of children, individuals not fully clothed, and couples engaged in sexual activities.

15. DesignerWare's servers send data captured by Detective Mode, unencrypted, directly to the email accounts designated by its licensees. DesignerWare's employees do not themselves view Detective Mode data, but without DesignerWare's licensing of PC Rental Agent and its making Detective Mode available to its licensees, as well as providing licensees with access to its web portal and providing servers to support both PC Rental Agent and Detective Mode, this collection and disclosure of private information would not be possible.

Complaint

Geophysical Location Tracking

16. Since at least September 2011, on every computer that has a wireless card installed, PC Rental Agent automatically logs the WiFi hotspots that the wireless card either sees or uses to connect to the Internet. When a computer connects to DesignerWare's servers, it reports the WiFi hotspot location information along with the computer's IP address.

17. DesignerWare cross-references the information logged by a rented computer to PC Rental Agent with a publicly available list of WiFi hotspots' physical locations and provides its licensees with street addresses for the particular WiFi hotspots viewed or accessed by the computer. The information derived from WiFi hotspot contacts can frequently pinpoint a computer's location to a single building, and, when aggregated, can track the movements and patterns of individual computer users over time. DesignerWare provides its licensees with this location information for the ten most recent reporting cycles. DesignerWare recommends that rent-to-own stores only use this data in connection with recovering stolen property, but it does not monitor, restrict, or otherwise limit its licensees' access to such location information.

18. DesignerWare applied its location tracking upgrade of PC Rental Agent to every computer on which PC Rental Agent was installed, without obtaining consent from, or providing notice to, the computers' renters. After the September 2011 upgrade, in numerous instances PC Rental Agent has been installed on rented computers without the computer renter's knowledge or consent. Thus, consumers using those computers on which PC Rental Agent is installed – who may or may not be the computers' renters, and who may or may not be current in their lease payments – do not know that their physical location can be identified from the WiFi hotspots that their computers encounter. Nor do they know that employees of the rent-to-own stores from which their computers are rented can monitor their physical locations and the patterns of their movements.

Complaint

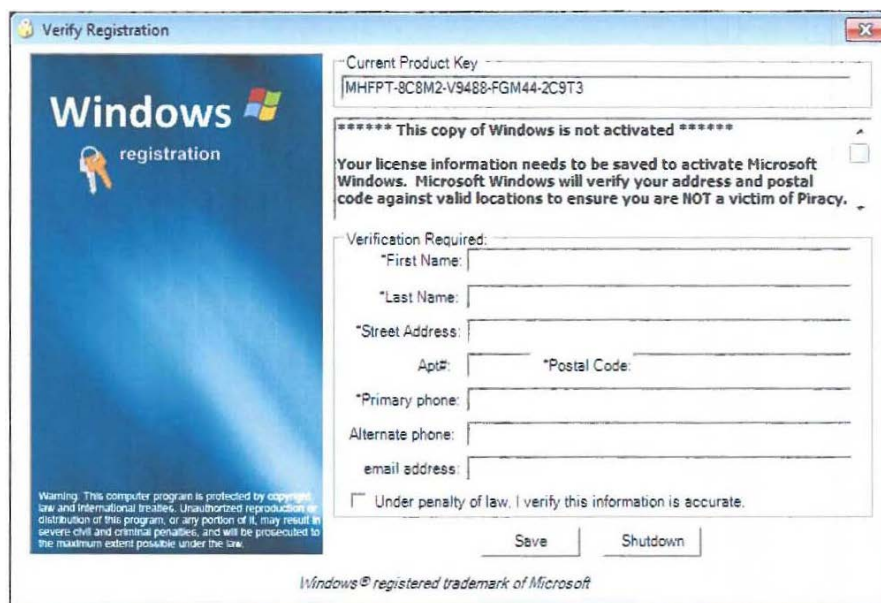
Substantial Injury

19. DesignerWare's collection and disclosure to third parties of private and confidential information about consumers, including both those who rented the computer and those who are merely using it, causes or is likely to cause substantial harm to consumers. Because of DesignerWare's intrusions, consumers are at risk of harm from the exposure of personal, financial account access, and medical information to strangers. Consumers are harmed by DesignerWare's unwarranted invasion into their homes and lives and its capture of the private details of individual and family life, including, for example, images of visitors, children, family interactions, partially undressed individuals, and couples engaged in intimate activities. Sharing these images with third parties can cause consumers financial and physical injury and impair their peaceful enjoyment of their homes. Consumers cannot reasonably avoid these injuries because PC Rental Agent is invisible to them. The harm caused by respondents' unauthorized collection and disclosure of confidential consumer information is not outweighed by countervailing benefits to consumers or to competition; indeed in this context, where rent-to-own stores have alternate effective methods of collection, including, e.g., using PC Rental Agent to remotely disable the computer, there are no legitimate benefits to respondents or to the public.

Detective Mode's Deceptive Prompt Windows

20. In addition to its other features, Detective Mode offers licensees the option to cause a user's computer to display a fake software registration window. The fake registration window prompts the computer user to enter a name, address, email address, and phone number. The computer user cannot close the window until the requested information is entered. DesignerWare has created several different fake registration windows for its licensees' use, including ones for Microsoft Windows, Internet Explorer, Microsoft Office, and Yahoo! Messenger, and one to verify a security certificate. A screenshot of DesignerWare's fake Microsoft Windows screen appears below.

Complaint



21. No actual software is registered as a result of a consumer providing the requested information; instead, Detective Mode captures the information entered in the prompt boxes and transmits it to DesignerWare, and DesignerWare's servers email the data to the rent-to-own store licensee, unbeknownst to the consumer.

22. Consumers who are deceived into providing contact information in this manner are deprived of the ability to control who has access to their contact information and how they are contacted.

VIOLATIONS OF THE FTC ACT**COUNT I****UNFAIR GATHERING AND DISCLOSURE OF
CONSUMERS' PERSONAL INFORMATION**

23. Through the means described in Paragraphs 5 through 22, in numerous instances respondents have:

- a. Installed monitoring software on rented computers, gathered sensitive personal, financial, and medical

Complaint

information about consumers from those computers, and disclosed that personal information to rent-to-own store licensees; and

- b. Installed geophysical location tracking software on rented computers without consent from the computers' renters, tracked the geophysical location of computers without notice to the computer users, and disclosed that location information to rent-to-own store licensees.

24. Respondents' actions cause 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.

25. Therefore, respondents' practices, as described in Paragraph 23, constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

**COUNT II
MEANS AND INSTRUMENTALITIES
TO ENGAGE IN UNFAIRNESS**

26. Through the means described in Paragraphs 5 through 22, respondents have:

- a. Furnished rent-to-own stores with software for installation on rented computers that i) when activated remotely by the rent-to-own store licensee will record keystrokes typed on a computer, capture screenshots of information displayed on a computer, cause a computer's webcam to take pictures of the computer user, and transmit the recorded keystrokes, screenshots and web pictures to the rent-to-own store licensee to view, and ii) will identify the geophysical location of the computer and track the physical location of the computer's user without consent from the computer's renter or notice to the computer's user; and

Complaint

- b. Provided rent-to-own store licensees with information improperly gathered from consumers for use in connection with collecting or attempting to collect a debt, money, or property pursuant to a consumer rental contract.

27. By furnishing others with the means to engage in the unfair practices described in Paragraph 26, respondents have provided the means and instrumentalities for the commission of unfair acts and practices and thus 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.

28. Therefore, respondents' practices, as described in Paragraph 26, constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT III
DECEPTIVE GATHERING AND DISCLOSURE OF
CONSUMERS' PERSONAL INFORMATION

29. Through the means described in Paragraphs 5 through 22, respondents have represented to consumers, expressly or by implication, that certain pop-up notices that appear on a computer's screen are notices from trusted software providers that contain software registration forms that must be filled out with the consumers' contact information in order to continue to use the providers' software.

30. In truth and in fact, these pop-up notices are not from trusted software providers and do not contain software registration forms that must be filled out with the consumers' contact information in order to continue to use the providers' software, but instead serve only to cause the consumer to provide the requested contact information so that it may be provided to respondents' rent-to-own store licensees.

Decision and Order

31. Therefore, respondents' practices, as described in Paragraph 29, constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this eleventh day of April, 2013, has issued this complaint against respondents.

By the Commission, Commissioner Wright not participating.

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 a consent order ("consent agreement"), an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said consent agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated as alleged in the complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and

Decision and Order

having thereupon accepted the executed consent agreement and placed such consent agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent DesignerWare, LLC (“DesignerWare”), is a Nevada limited liability corporation with its principal office or place of business at 108 Hutchinson Drive, North East, Pennsylvania 16428.
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:

1. Unless otherwise specified, “respondent” shall mean DesignerWare and its successors and assigns.
2. “Commerce” shall be defined as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “Computer” shall mean any desktop or laptop computer, handheld device, tablet, telephone, 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.
4. “Clear(ly) and prominent(ly)” shall mean:
 - a. In textual communications (e.g., printed publications or words displayed on the screen of a

Decision and Order

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;

- b. 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;
 - c. 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;
 - d. 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
 - e. 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.
5. “Geophysical location tracking technology” shall mean any hardware, software, or application utilized in conjunction with a computer that collects and reports data or information that identifies the precise

Decision and Order

geophysical location of the computer. Geophysical location tracking technologies include, for these purposes, technologies that report: the GPS coordinates of a computer; 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 through geolocation lookup services; or any information derived from any combination of the foregoing.

6. “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:
 - a. Recording keystrokes, clicks, or other user-generated actions;
 - b. Capturing screenshots of the information displayed on a computer monitor or screen; or
 - c. Activating the camera or microphone function of a computer to take photographs or record audio or visual content through the computer’s webcam or microphone.
7. “Covered rent-to-own transaction” shall mean any transaction where a consumer enters into an agreement for the purchase or rental of a computer and the consumer’s contract or rental agreement provides for payments over time and an option to purchase the computer.

Decision and Order

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 it who receive actual notice of this order, by personal service or otherwise, in connection with using, selling, licensing, or otherwise providing any hardware, software, application, program, or other device for use in connection with a covered rent-to-own transaction, directly or indirectly, is hereby permanently restrained and enjoined from:

- A. Using any monitoring technology to gather information or data from any computer rented to a consumer; and
- B. Licensing, selling, or otherwise providing third parties with monitoring technology for installation or activation on computers rented to consumers.

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 it who receive actual notice of this order, by personal service or otherwise, in connection with using, selling, licensing, or otherwise providing any hardware, software, application, program, or other device for use in connection with a covered rent-to-own transaction, directly or indirectly, is hereby permanently restrained and enjoined from:

- A. Gathering any information or data from any computer via any geophysical location tracking technology without ensuring that the computer user is provided clear and prominent notice at the time the computer is rented and immediately prior to each use of the

Decision and Order

geophysical location tracking technology, and also ensuring that the computer renter's affirmative express consent is obtained at the time the computer is rented. For purposes of this section, providing clear and prominent notice to computer users and obtaining affirmative express consent from computer renters means:

1. Clear and Prominent Notice: a clear and prominent notice is provided 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 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;
2. Affirmative Express Consent: affirmative express consent is obtained by giving the computer 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 setting. Activation of any geophysical location tracking technology must not proceed until the computer's renter provides affirmative express consent. Notwithstanding the foregoing, nothing in this Part shall require that a computer be rented to a user who declines to consent to installation or activation of any geophysical tracking technology;
3. Icons: the activation of any geophysical location tracking technology shall be accompanied by the installation of a clear and prominent icon on the

Decision and Order

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 the notice requirements of this Part may be suspended and geophysical location tracking technology activated if (a) the renter reports that the computer has been stolen or there is otherwise a reasonable basis to believe that the computer has been stolen, and (b) either the renter or another person has filed a police report stating that the computer has been stolen. *Provided further that* respondent shall ensure that documents establishing (a) and (b) are retained. For purposes of this Order, “filing of a police report” means the reporting of a complaint with the police department in any form recognized in the jurisdiction;

Provided further that the notice and record-keeping requirements of this Section II shall be satisfied when respondent acts as a licensor if respondent includes in the licensing agreement contractual requirements that: (i) licensees may only activate geophysical location tracking technology if (a) the renter reports that the computer has been stolen or there is otherwise a reasonable basis to believe that the computer has been stolen and (b) either the renter or another person has filed a police report stating that the computer has been stolen, and (ii) documents establishing (a) and (b) are retained by the licensees; and

Decision and Order

- B. Licensing, selling, or otherwise providing any third party with geophysical location tracking technology for installation or activation on a computer to be rented in a covered rent-to-own transaction, without requiring as a condition of the license, sale, or other provision of the technology that the third party obtain consent and provide notice as provided in Section II.A, above.

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 it who receive actual notice of this order, by personal service or otherwise, in connection with using, selling, licensing, or otherwise providing any hardware, software, application, program, or other device, is hereby permanently restrained and enjoined from making, or assisting others to make, 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 information from or about a consumer, including without limitation location information.

IV.
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 it who receive actual notice of this order, by personal service or otherwise, shall:

- A. Delete or destroy all user data, if any, previously gathered 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

Decision and Order

- B. Transfer data or information, if any, 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 only if such information is rendered unreadable, unusable, or indecipherable during transmission.

V.**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 using, selling, licensing, or otherwise providing any hardware, software, application, program, or other device, directly or indirectly, 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 personal information gathered from or about consumers.

VI.**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 current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. From each person 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

Decision and Order

signatures complying with the requirements of the E-Sign Act, 15 U.S.C. § 7001 et seq.

VII.
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, they 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.
- 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,

Decision and Order

with the subject line DesignerWare, LLC, File No. 1123151. *Provided, however;* that, in lieu of overnight courier, notices may be sent by first class mail, but only if an electronic version of each such notice is contemporaneously sent to the Commission at DEbrief@ftc.gov.

**VIII.
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 – V 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 any monitoring or geophysical tracking technologies sold, licensed, or otherwise provided to any third party for use in connection with any covered rent-to-own transaction, 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 VI.

Analysis to Aid Public Comment

**IX.
TERMINATION OF ORDER**

This Order will terminate on April 11, 2033, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this Order that terminates in less than twenty (20) years;
- B. This Order 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, Commissioner Wright not participating.

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

The Federal Trade Commission (“Commission” or “FTC”) has accepted, subject to final approval, consent agreements from the following respondents: DesignerWare, LLC; Timothy Kelly, and Ronald P. Koller, individually and as officers of DesignerWare, LLC; Aspen Way Enterprises, Inc.; Watershed Development Corp.; Showplace, Inc., d/b/a Showplace Rent-to-Own; J.A.G. Rents, LLC, d/b/a ColorTyme; Red Zone, Inc., d/b/a

Analysis to Aid Public Comment

ColorTyme; B. Stamper Enterprises, Inc., d/b/a Premier Rental Purchase; and C.A.L.M. Ventures, Inc., d/b/a Premier Rental Purchase.

The proposed consent orders have 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 agreements and the comments received, and will decide whether it should withdraw from any of the agreements and take appropriate action or make final the agreements' proposed orders.

Timothy Kelly and Ronald Koller founded and co-owned DesignerWare, LLC, a small software company that designed and licenses a single product, PC Rental Agent. Mr. Koller ended his association with DesignerWare in March 2012. PC Rental Agent is exclusively marketed to rent-to-own ("RTO") stores. RTO stores rent to consumers a variety of household items, including personal computers. PC Rental Agent is designed to assist RTO stores in tracking and recovering rented computers. Its chief function is a "kill switch," a program that can be used by a store to render a computer inoperable if the consumer renter is late or defaults on payments or if the computer is stolen. PC Rental Agent also offers a wiping feature that permits RTO stores to quickly erase the hard drives of computers prior to re-renting them to consumers.

Through PC Rental Agent, which RTO store licensees installed on rented computers, DesignerWare also provided access to "Detective Mode." Detective Mode was a software application embedded in the PC Rental Agent program. At the request of an RTO store, DesignerWare would remotely complete the Detective Mode installation process on an individual computer and activate "the Detective." Detective Mode would surreptitiously log the computer user's keystrokes, capture screenshots, and take pictures with the computer's webcam and send the data to DesignerWare's servers. Neither DesignerWare nor the RTO stores who have used Detective Mode disclosed to computer users that they were being monitored in this manner. Although DesignerWare recommended that Detective Mode be installed and activated only

Analysis to Aid Public Comment

to locate and identify the person in possession of a lost or stolen computer, DesignerWare did not monitor its own collection of or limit RTO stores' access to Detective Mode information to ensure that the information was obtained and used only for designated purposes.

DesignerWare sent the information captured by Detective Mode to an email account designated by each RTO store. Although DesignerWare's employees did not themselves view Detective Mode data, without DesignerWare licensing PC Rental Agent and making Detective Mode available to the RTO stores, as well as providing them with access to its web portal and providing servers to support both PC Rental Agent and Detective Mode, this collection and disclosure of consumers' private information would not be possible.

RTO stores also used Detective Mode to send fake "software registration" forms to consumers to deceive them into providing their contact and location information. DesignerWare created several different fake registration forms that its servers displayed on consumers' computers. An RTO store could use this feature of Detective Mode by requesting that DesignerWare activate it. No actual software was registered as a result of a consumer providing the requested information. Rather, Detective Mode captured the information entered in the prompt boxes and sent it to DesignerWare, who then emailed the data to the RTO store, all unbeknownst to the consumer. DesignerWare discontinued use of Detective Mode in January 2012.

In September 2011, DesignerWare added another feature to PC Rental Agent: the capacity to track the physical location of rented computers via WiFi hotspot locations. The information derived from WiFi hotspot contacts can frequently pinpoint a computer's location to a single building and, when aggregated, can track the movements and patterns of individual computer users over time. DesignerWare makes this information easily available to the RTO stores by cross-referencing a list of publicly available WiFi hotspots with the street addresses for the particular hotspots viewed or accessed by rented computers. DesignerWare applied its location tracking upgrade of PC Rental Agent to every computer on which PC Rental Agent was installed, without obtaining consent from, or providing notice to, the computers'

Analysis to Aid Public Comment

renters. DesignerWare recommends that RTO stores only use this tracking data in connection with recovering stolen property, but it does not monitor or limit the RTO stores' access to such location information.

Aspen Way Enterprises, Watershed Development, Showplace, J.A.G. Rents, Red Zone, B. Stamper Enterprises, and C.A.L.M. Ventures are RTO stores that have licensed PC Rental Agent from DesignerWare. These RTO stores have used information transmitted by DesignerWare when attempting to collect from computer renters who are late in paying or have otherwise breached their rental contracts. Using Detective Mode, these RTO stores have received from DesignerWare webcam photos of computer users (and anyone else within view of the camera), computer users' keystrokes, and screenshots of their computer activities. This information has revealed private and confidential details about computer users, such as their passwords for access to email accounts, social media websites, and financial institutions. Other confidential information was also captured, including medical records, private emails to doctors, employment applications containing Social Security numbers, bank and credit card statements, and discussions of defense strategies in a pending lawsuit. Through Detective Mode, DesignerWare and the RTO stores also secretly photographed the private conduct of consumers in their homes. This included pictures of children, household visitors, individuals not fully clothed, and couples engaged in intimate activities.

The collection and disclosure of such private and confidential information about consumers causes or is likely to cause substantial injury to consumers. Consumers are likely to be substantially injured by the exposure to strangers of personal, financial account access, and medical information. Consumers are actually harmed by DesignerWare's unwarranted invasion into their homes and lives and its capture and disclosure of the private details of individual and family life, including, for example, images of visitors, children, family interactions, partially undressed individuals, and couples engaged in sexual activities. Sharing data like that collected by Detective Mode with third parties can cause consumers financial and physical injury, and impair their peaceful enjoyment of their homes. Because

Analysis to Aid Public Comment

Detective Mode functions secretly, consumers cannot reasonably avoid this harm, which is neither trivial nor speculative. Moreover, there are no countervailing benefits to consumers or competition for continued use of Detective Mode in this context, where RTO stores have effective alternative methods for collections.

DesignerWare also sent consumers' contact information to the RTO stores. DesignerWare gathered this information from computer users who completed the deceptive "software registration" forms sent through Detective Mode. The RTO stores used this information to find, require payment for, or repossess a rented computer.

The Commission's complaint against DesignerWare, Kelly, and Koller (collectively, "DesignerWare Respondents") alleges that the company and its principals engaged in unfair and deceptive conduct and provided the means and instrumentalities to engage in unfairness, all in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. The first count of the complaint focuses on actions taken by DesignerWare that caused or was likely to cause substantial injury to consumers. Count I alleges that the DesignerWare Respondents engaged in unfair conduct by installing monitoring software on rented computers, gathering personal, financial, and health information about consumers from computers, and disclosing that information to RTO store licensees. Count I also alleges as unfair the DesignerWare Respondents' installation of geophysical location tracking software on rented computers without consent from the computer renters, the tracking of computers' geophysical locations without notice to computer users, and the disclosure of that information to the RTO stores.

Count II alleges that the DesignerWare Respondents provided the means to third parties – the RTO stores – to violate Section 5. The first part of the count charges the DesignerWare Respondents with providing RTO stores with the means and instrumentalities to engage in unfairness by furnishing them with software that could monitor consumers by recording their keystrokes, capturing screenshots of information displayed on a computer, and taking pictures of the computer user, and further could track the geophysical location data of rented computers without the consent

Analysis to Aid Public Comment

of the computer renter or notice to the computer user. The second part of Count II alleges that the DesignerWare Respondents provided the means and instrumentalities to RTO stores to engage in unfair collection practices by providing them with the data gathered via PC Rental Agent and Detective Mode. Count II focuses on actions taken by DesignerWare that were integral to the harm to consumers caused or likely to be caused by the RTO stores. Here, without PC Rental Agent and Detective Mode and without access to DesignerWare's servers to execute their commands to rented computers, collect consumers' confidential information and transmit it to them, the RTO stores could not unfairly monitor their computer renters or use improperly gathered information in connection with collections.

Count III of the complaint charges the DesignerWare Respondents with deceptively gathering – and disclosing – consumers' personal information collected from the fake software registration forms that Detective Mode caused to appear on consumers' rented computers.

Each of the Commission's complaints against the seven RTO stores contains substantially similar allegations regarding the stores' violations of the FTC Act. The complaints charge that the RTO stores unfairly gathered consumers' personal information by installing monitoring software on rented computers and engaged in unfair collection practices by using the improperly gathered information to collect on consumer rental contracts. The complaints further allege that the RTO stores deceptively gathered consumers' personal information by activating the Detective Mode feature that sends the fake software registration forms to consumers' rented computers.

The proposed orders contain strong injunctive relief designed to remedy the unlawful conduct by DesignerWare, its principals, and the RTO stores. The orders define "monitoring technology and geophysical location tracking technology" so that the technological applications covered by the order are clearly described. "Monitoring technology" means 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 recording

Analysis to Aid Public Comment

keystrokes, clicks, or other user-generated actions; capturing screenshots of the information displayed on a computer monitor or screen; or activating the camera or microphone function of a computer to take photographs or record audio or visual content through the computer's webcam or microphone. The definition of "geophysical location tracking" includes the reporting of GPS coordinates, WiFi hotspots, or telecommunications towers – all technologies that allow for a relatively precise location of the item tracked. In addition, a "covered rent-to-own transaction" is defined as one in which a consumer agrees to purchase or rent a computer, where the rental agreement provides for payments over time and an option to purchase the computer.

The proposed orders with DesignerWare and its principals, Kelly and Koller, are separate, but contain identical injunctive provisions. Section I of the proposed orders with DesignerWare and its principals bans them from using – as well as licensing, selling, or otherwise providing third parties with – monitoring technology in connection with any covered RTO transaction. Section II prohibits them from using geophysical location tracking technology to gather information from any computer without providing clear and prominent notice to and obtaining affirmative express consent from the computer's renter at the time the computer is rented. This section also requires clear and prominent notice to computer users immediately prior to each time tracking technology is activated. In addition, Section II mandates that DesignerWare and its principals require their licensees to obtain consent and provide notice prior to initiating any location tracking. However, DesignerWare and its principals do not need to provide notice to a computer user prior to activating geophysical location tracking technology if 1) there is a reasonable basis to believe that the computer has been stolen and 2) a police report has been filed.

Section III of the proposed orders with DesignerWare and its principals prohibits the deceptive collection of consumer information via fake software registration notices. Section IV requires that any data that was collected through any monitoring or tracking software without the requisite notice and consent be destroyed and that any properly collected data be encrypted when transmitted. Section V bars DesignerWare and its principals from

Analysis to Aid Public Comment

making misrepresentations about the privacy or security of any personal information gathered from or about consumers.

Sections VI through IX of both orders contain reporting and compliance provisions. Section VI of the proposed DesignerWare order requires the company to disseminate the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. This section also requires DesignerWare to secure a signed and dated statement acknowledging receipt of the order from all persons who receive a copy. Section VII requires DesignerWare to submit compliance reports to the Commission within sixty (60) days, and periodically thereafter as requested. It also requires the company to notify the Commission of changes in DesignerWare's corporate status.

Section VI of the proposed order with the DesignerWare principals requires respondents to distribute it to all current and future principals, officers, directors, and managers of any company that either respondent controls that engages in any covered RTO transaction as well as to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. It also requires the respondents to secure a signed and dated statement acknowledging receipt of the order from all persons who receive a copy. Section VII of the proposed order with the DesignerWare principals requires them to submit compliance reports to the Commission within sixty (60) days, and periodically thereafter as requested. In addition, this section requires them to notify the Commission of changes in their business or employment for three (3) years.

Under Section VIII of the proposed orders with both DesignerWare and its principals, respondents must retain documents relating to their compliance with the order for a five (5) year period. Finally, Section IX of both proposed orders is a provision "sunsetting" the orders after twenty (20) years, with certain exceptions.

The proposed orders against the RTO stores (which are identical to each other) contain similar injunctive provisions to

Analysis to Aid Public Comment

those in the proposed orders with DesignerWare and its principals. Section I of each of the proposed orders bans the RTO stores from using monitoring technology in connection with any covered RTO transaction. Section II prohibits the stores from using geophysical location tracking technology to gather information from any computer without providing clear and prominent notice to the computer's renter and obtaining affirmative express consent from the computer's renter at the time the computer is rented. This section also requires clear and prominent notice to a computer user immediately prior to each time such technology is activated. The proposed RTO store orders also suspend the notice requirement if 1) there is a reasonable basis to believe that the computer has been stolen and 2) a police report has been filed. Section III of each of the proposed orders prohibits the deceptive collection of consumer information via fake software registration notices.

Section IV bars the stores from collecting or attempting to collect a debt, money, or property pursuant to a consumer rental contract by using any information or data that was improperly obtained from a computer by monitoring technology. Section V requires that any data collected through any monitoring or tracking software without the requisite notice and consent be destroyed, and that any properly collected data be encrypted when transmitted. As fencing in, Section VI bars misrepresentations about the privacy or security of any personal information gathered from or about consumers.

Sections VII through X of the proposed RTO store orders contain reporting and compliance provisions. Section VII requires distribution of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. It also requires the RTO stores to secure signed and dated statements acknowledging receipt of the order from all persons who receive a copy of the order. Section VIII requires the RTO stores to submit compliance reports to the Commission within sixty (60) days, and periodically thereafter as requested, and ensures notification to the Commission of changes in corporate status. Under Section IX, the RTO stores must retain documents relating to order compliance for a five (5) year period.

Analysis to Aid Public Comment

Finally, Section X 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 orders. It is not intended to constitute an official interpretation of the proposed complaints or orders or to modify the terms of the orders in any way.

Complaint

IN THE MATTER OF

**TIMOTHY KELLY
AND
RONALD P. KOLLER**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4391; File No. 112 3151
Complaint, April 11, 2013 – Decision, April 11, 2013*

This consent order relates to privacy violations by Timothy Kelly and Ronald P. Koller (“Respondents”) in the licensing of its PC Rental Agent software application to rent-to-own (“RTO”) stores. Respondents founded and co-owned DesignerWare, LLC, a company that licensed a software program known as PC Rental Agent to RTO stores. The purpose of PC Rental Agent was to aid RTO stores in tracking and recovering rented computers; to render computers inoperable if consumers are late or default on payments or are stolen; and to erase computer hard drives for redistribution. The complaint alleges that DesignerWare, LLC and Respondents failed notify consumers that the PC Rental Agent application tracked the movements and patterns of individual computer users over time, or obtain their consent to such tracking, in violation of Section 5 of the Federal Trade Commission Act. The consent order requires Respondents to cease all use, license, and sale of monitoring technology in connection with RTO transactions.

Participants

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

For the *Respondents*: Stephen S. Stallings, Burns White LLC, and William Woodward Webb, Edmisten & Webb Law Firm. .

COMPLAINT

The Federal Trade Commission, having reason to believe that DesignerWare, LLC, a corporation, and Timothy Kelly and Ronald P. Koller, individually and as officers of the corporation (“respondents”), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges: