Analysis of Proposed Consent Orders to Aid Public Comment
In the Matter of DesignerWare, LLC, et al., File No. 1123151

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 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 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' 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 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 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 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 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 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. 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.