

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
J. Thomas Rosch
Edith Ramirez
Julie Brill
Maureen K. Ohlhausen

In the Matter of)	
)	
DESIGNERWARE, LLC,)	
a limited liability corporation;)	DOCKET NO.
TIMOTHY KELLY, individually)	
and as an officer of the corporation; and)	
RONALD P. KOLLER, individually)	
and as an officer of the corporation)	

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:

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.

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.

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 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.

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

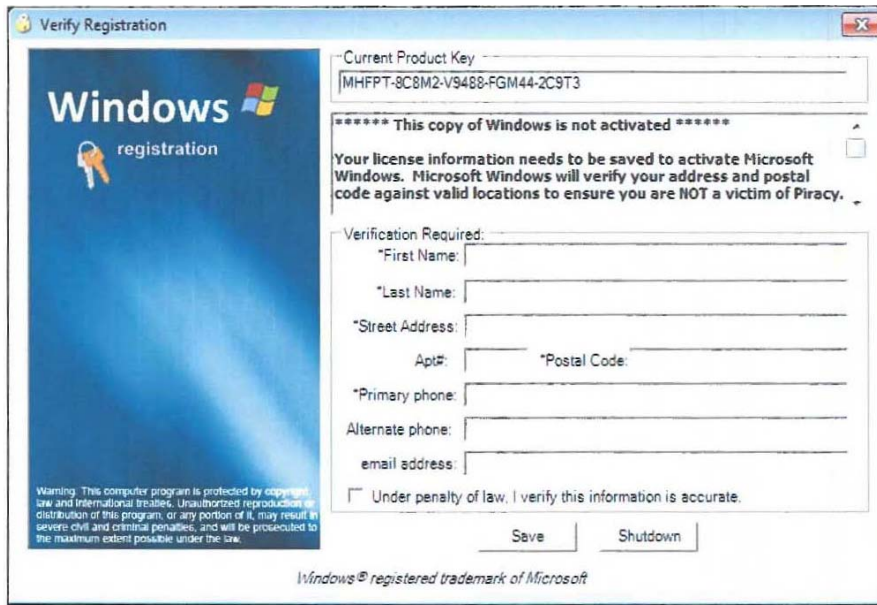
that their computers encounter. Nor do they know that employees of the rent-to-own stores from which their computers are rented can monitor their physical locations and the patterns of their movements.

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.



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 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

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 consumer's 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 consumer's 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.

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 ___ day of ____, 2012, has issued this complaint against respondents.

By the Commission.

Donald S. Clark
Secretary