**152 3159**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:** **Edith Ramirez, Chairwoman**
**Maureen K. Ohlhausen**
**Terrell McSweeny**

**In the Matter of**

**GENERAL WORKINGS INC., a corporation, also d/b/a VULCUN, and**

**ALI MOIZ and MURTAZA HUSSAIN, individually and as officers of GENERAL WORKINGS, INC.**

**DOCKET NO. C-4573**

# COMPLAINT

The Federal Trade Commission, having reason to believe that General Workings Inc., a corporation, and Ali Moiz and Murtaza Hussain, individually and as officers of the corporation (collectively "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 General Workings Inc., also doing business as Vulcun ("Vulcun"), is a Delaware corporation with its principal office or place of business at 424 Clay Street, San Francisco, California 94111.

*2.* Respondent Ali Moiz is a founder and officer of Vulcun. Individually or in concert with others, he controlled or had the authority to control, or participated in, the acts and practices of Vulcun, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Vulcun.

3. Respondent Murtaza Hussain is a founder and officer of Vulcun. Individually or in concert with others, he controlled or had the authority to control, or participated in, the acts and practices of the Vulcun, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Vulcun.

4. As described below, Respondents installed software, including Chrome browser extensions and mobile apps, onto users' desktops and mobile devices without adequately disclosing to users that the software would be installed. Respondents' conduct had two parts.

First, Respondents acquired a popular browser-based game called *Running Fred* and replaced it entirely with their own software program, called *Weekly Android Apps*, on users' desktops. Users of *Running Fred* were not informed that the game had been replaced. Second, *Weekly Android Apps* contained code that would install, again without adequate disclosure to users, apps on user's mobile devices.

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

## Desktop Computer Browser Extensions

6. Google, Inc. ("Google") offers a web browser, Chrome, as a free download for desktop computer and mobile operating systems. The desktop-computer version of Chrome allows users to install "extensions," which are software programs that can modify and extend Chrome's functionality. Extensions are created using web technologies like HTML, JavaScript, and Cascading Style Sheets. Extensions can perform minimal functions in the browser, like displaying the number of unread emails in a user's account. But they also can operate as complete, independent programs. Among the available Chrome browser extensions are games, news readers, video-streaming clients, project-management applications, and many others. Chrome browser extensions currently run only in the desktop-computer version of Chrome; the version of Chrome for mobile operating systems does not allow the use of extensions.

7. The Chrome Web Store is Google's portal for consumers to find and install extensions in their Chrome web browser. Similar to a mobile-app store like the Google Play Store, the Chrome Web Store allows users to view information about extensions that are offered by developers and also to install those extensions. The Chrome Web Store displays, for example, user reviews and ratings of available Chrome browser extensions. The Chrome Web Store also displays the number of users who have installed each extension. When users comment or review an extension, it is possible for the developer of the extension to write a response to the review. These reviews, and any responses, are then visible to consumers browsing the Chrome Web Store.

## Installation of Mobile Apps

8. The Google Play Store is Google's portal for consumers to find and install apps on devices running the Android mobile operating system. The Google Play Store is accessible through a website on a desktop-computer browser and through a standalone Android app.

9. Some users can only install mobile apps from their mobile devices. Other users have configured their accounts to allow their desktop computers, through the Google Play Store, to install Android apps on their mobile devices.

10. When users install a mobile app (whether they do so from a desktop computer or mobile device), the user is presented with a window describing what information, including sensitive information (*e.g.*, location information) or sensitive device functionality (*e.g.*, the ability to take

photos with the device's camera), an app may access. The installation process allows users to decline to install an app if they do not wish to grant the app's requested permissions.

## The Takeover of *Running Fred*

11. Chrome browser extensions are associated in the Chrome Web Store with particular developers or other entities. Dedalord, LLC, a game developer, offered a browser extension, *Running Fred*, in the Chrome Web Store. *Running Fred* became a popular Chrome-extension game with a large number of users. *Running Fred* had more than 200,000 users and an average star rating of 4.5 stars (out of 5 possible stars) with approximately 2,300 reviews.

12. On or around September 9, 2014, Respondents acquired control of *Running Fred.* Shortly thereafter, Respondents replaced *Running Fred* on these users' browsers with another Chrome browser extension called *Weekly Android Apps*. The users of *Running Fred* were not notified that *Running Fred* had been replaced.

## Respondents' Advertising of *Weekly Android Apps*

13. After replacing *Running Fred* with *Weekly Android Apps*, Respondents continued to advertise and distribute Chrome Extensions called *Weekly Android Apps* and *Apps by Cindy* to consumers via the Chrome Web Store. In the Chrome Web Store, Respondents stated that *Weekly Android Apps* offered consumers "the hottest mobile apps." Moreover, Respondents claimed the apps selected would be "hand picked" and not influenced by payments from developers. Exhibit A (screen shot from Chrome Web Store). In fact, Respondents did accept payments from at least one developer of an apps that was included in *Weekly Android Apps*. Respondents also claimed—inaccurately—that their extensions, which includes *Weekly Android Apps*, had been featured on prominent tech sites, such as MacRumors, Engadget, and Lifehacker. Further, Respondents claimed—again inaccurately—that *Apps by Cindy* had been selected as "one of the best mobile blogs of 2013" by RunMobile.

14. Consumers often install extensions based on the popularity and star rating of Chrome browser extensions in the Chrome Web Store. After the takeover of *Running Fred*, the information page for *Weekly Android Apps* on the Chrome Web Store stated that it had more than 200,000 users, 2,300 reviews, and an average 4.5-star-rating. Exhibit B (screen shot from Chrome Web Store). This user count and star rating, however, primarily reflected the user count and star rating associated with *Running Fred*. Few, if any of, these users had ever rated or used *Weekly Android Apps*.

## Disruption of Users' Experience on Mobile Devices and Desktop Computers

15. Once installed on users' desktop computers, *Weekly Android Apps* force-installed apps onto those users' mobile devices. *Weekly Android Apps* accomplished this by preventing users from reviewing the Android permissions associated with the apps that it installed onto users' mobile devices. These permissions would have shown the user what information or device functionality the apps could access. Code in *Weekly Android Apps* hid these permissions and

automatically approved the default Android permissions request associated with the apps without the user's knowledge. *Weekly Android Apps*, after taking over *Running Fred*, installed numerous apps using this code, including one solitaire game and a second app called *myphoneemails*.

16. *Weekly Android Apps* significantly disrupted users' operation of their desktop computers. *Weekly Android Apps* opened additional windows and also reset the users' home page for their browsers. Desktop-computer users saw new tabs or windows open repeatedly. When users closed the new windows, others would pop up. One user complained that "[t]his was installed automatically somehow, it has something to do with a . . . bug that has infected my chromebook[.] [O]n [C]hrome I have tabs opening by themselves advertising this poker and other [P]lay [S]tore items saying 'click here to install on your phone[.]' I have never authorized this tab[.] Please stop these people!!!!" Another user stated that "I didn't ask for this extension to be installed, and there was no notification that it was being installed, yet it just showed up in my browser! I only found out about it because Chrome informed me that it was taking over my home page! How did this happen?"

17. *Weekly Android Apps* also significantly disrupted users' operation of their mobile devices without appropriate consent. Once *Weekly Android Apps* was installed on user's desktop browsers, it would redirect the users' browsers to the Google Play Store. Once at the Google Play Store, *Weekly Android Apps* would detect and click the "Buy" buttons associated with certain mobile apps without notifying the user. *Weekly Android Apps* would also accept the Android permission notification without notifying the user. As a result, mobile-device users found unexpected and unfamiliar apps on their devices, and, when users sought to delete those apps, new ones reappeared, without any action from the users. One user complained that the mobile app "keeps reinstalling itself. . . . It's happening to my wife's phone too. Help!" Another user complained that "[i]t continuously installs itself to my system without my consent no matter how many times I try to uninstall it. Others are also experiencing this. This 'application' might be a virus."

18. Because the *Weekly Android Apps* hid and accepted the default Android permissions request, these mobile apps could have gained immediate access to the user's address book, photos, location, and persistent device identifiers. In addition, once installed, the apps could have gained access to other information, including financial and health information, by executing additional malicious code on the consumer's mobile device.

**COUNT I**
Unfair Practice

19. As described in paragraphs 11 through 18, Respondents installed *Weekly Android Apps* on more than 200,000 users' browsers without adequate notice to the users or consent for the installation. Users whose desktop and mobile devices were compromised had their experience of using their devices seriously disrupted. Moreover, *Weekly Android Apps* allowed Respondents to force-install apps onto users' mobile devices. The force-installed apps on

users' mobile devices also repeatedly reappeared after users attempted to remove them. These actions seriously interfered with the consumers' use of their desktop computers and mobile devices. In addition, any apps force-installed on users' mobile devices could have provided Respondents and the app developer with access to private, sensitive information stored on the users' mobile devices, including user's address book, photos, location, persistent device identifiers, and medical and financial information. Respondents' conduct has caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Respondents' conduct is an unfair act or practice.

**COUNT II**
False Claims

20. In connection with the advertising, promotion, or distribution of *Weekly Android Apps*, Respondents have represented, directly or indirectly, expressly or by implication, that:

A. *Weekly Android Apps* provides impartial, independent selections of apps.

B. *Weekly Android Apps* has been featured on prominent tech sites, such as MacRumors, Engadget and Lifehacker.

C. *Apps by Cindy* has been selected as one of the best mobile blogs of 2013 by RunMobile.

D. *Weekly Android Apps* has been installed by more than 200,000 users.

E. *Weekly Android Apps* had more than 2,300 reviews and an average rating of 4.5 out of 5 stars.

21. In truth and in fact:

A. *Weekly Android Apps* did not provide impartial, independent selections of apps. Respondents received some financial compensation in return for installing the developers' apps on consumers' mobile devices.

B. *Weekly Android Apps* had not been featured on prominent tech sites such as MacRumors, Engadget, and Lifehacker.

C. *Apps by Cindy* has not been selected as one of the best mobile blogs of 2013 by RunMobile.

*D.* *Weekly Android Apps* had not been installed by more than 200,000 users. Rather, the vast majority of these users had installed *Running Fred*, not *Weekly Android Apps*.

E. *Weekly Android Apps* did not have more than 2,300 reviews and an average rating of 4.5 out of 5 stars. The vast majority of these ratings were from *Running Fred* users, not *Weekly Android Apps* users.

22. Therefore, the representations set forth in Paragraph 20 were, and are, false and misleading.

## Violations of Section 5

23. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

**THEREFORE**, the Federal Trade Commission this eighteenth day of April, 2016, has issued this complaint against Respondents.

By the Commission.

Donald S. Clark
Secretary

SEAL: