142 3156

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

	)	
In the Matter of	)	**DOCKET NO. C-4587**
	)	
ASUSTeK Computer, Inc.,	)	
a corporation.	)	
	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that ASUSTeK Computer, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent ASUSTeK Computer, Inc. is a Taiwanese corporation with its principal office or place of business at 15, Li-Te Rd., Peitou, Taipei 11259, Taiwan.

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

RESPONDENT'S BUSINESS PRACTICES

3. Respondent ASUSTeK Computer, Inc. ("ASUS") is a hardware manufacturer that, among other things, sells routers, and related software and services, intended for consumer use. ASUS designs the software for its routers, controls U.S. marketing and advertising for its routers, including on websites targeting U.S. consumers, and is responsible for developing and distributing software updates to remediate security vulnerabilities and other flaws in routers sold to U.S. consumers. ASUS sells its routers in the United States through a wholly owned U.S. subsidiary, which distributes the routers for sale through third-party retailers, in stores and online, throughout the United States.

RESPONDENT'S ROUTERS AND "CLOUD" FEATURES

4. Routers forward data packets along a network. In addition to routing network traffic, consumer routers typically function as a hardware firewall for the local network, and act as the first line of defense in protecting consumer devices on the local network, such as computers, smartphones, internet-protocol ("IP -

10.

Insecure Design

15. Consumers could set up an AiDisk FTP server in two ways. The first was through a set of menus called the "AiDisk wizard." During setup, the AiDisk wizard asks the consumer to "Decide how to share your folders," and presents three options: "limitless access rights," "limited access rights," and "admin rights." Prior to January 2014, the AiDisk wizard did not provide consumers with sufficient information to evaluate these options, and pre-selected the "limitless access rights" option for the consumer (*see* Exh. F, p. 1 of 2). If the consumer completed setup with this default option in place, the AiDisk wizard created an FTP server that would provide anyone on the internet who had the router's IP address with unauthenticated access to the consumer's USB storage device.

16. The second way consumers could set up an AiDisk FTP server was through a submenu in the admin console called "USB Application – FTP Share." The submenu did not provide consumers with any information regarding the default settings or the alternative settings that were available. If a consumer clicked on the option to "Enable FTP" (*see* Exh. G, p. 1 of 2), the software created an AiDisk FTP server that, by default, provided anyone on the internet who had the router's IP address with unauthenticated access to the consumer's USB storage device.

17. Neither set-up option provided any explanation that the default settings would provide anyone on the internet with unauthenticated access to all of the files saved on the consumer's USB storage device. And in both cases, search engines could index any of the files exposed by these unauthenticated FTP servers, making them easily searchable online.

18. If a consumer wanted to prevent unauthenticated access through the AiDisk wizard, the consumer needed to deviate from the default settings and select "limited access rights." The consumer would then be presented with the option to create login credentials for the

25. For example, the admin console has been susceptible to pervasive cross-site request forgery ("CSRF") vulnerabilities that would allow an attacker to force malicious changes to any of the router's security settings (*e.g.*, disabling the firewall, enabling remote management, allowing unauthenticated access to an AiDisk server, or configuring the router to redirect the consumer to malicious websites) without the consumer's knowledge. Despite the serious consequences of these vulnerabilities, respondent did not perform pre-release testing for this class of vulnerabilities. Nor did respondent implement well-known, low-cost measures to protect against them, such as anti-CSRF tokens – unique values added to requests sent between a web application and a server that only the server can verify, allowing the server to reject forged requests sent by attackers.

26. Beginning in March 2013, respondent received multiple reports from security researchers regarding the CSRF vulnerabilities affecting respondent's routers. Despite these reports, respondent took no action to fix the vulnerabilities for at least a year, placing consumers' routers at risk of exploit. Indeed, in April 2015, a malware researcher discovered a large-scale, active CSRF exploit campaign that reconfigured vulnerable routers so that the attackers could control and redirect consumers' web traffic. This exploit campaign specifically targeted numerous ASUS router models.

FIRMWARE UPGRADE TOOL

27. The admin console includes a tool that ostensibly allows consumers to check whether their router is using the most current firmware ("firmware upgrade tool"). When consumers click on the "Check" button, the tool indicates that the "router is checking the ASUS server for the firmware update" (*see* Exh. H).

28. In order for the firmware upgrade tool to recognize the latest available firmware, ASUS must update a list of available firmware on its server. On several occasions, ASUS has failed to update this list. In July 2013, respondent received reports that the firmware upgrade tool was not recognizing the latest available firmware from both a product review journalist and by individuals calling into respondent's customer-support call center. Likewise, in February 2014, a security researcher notified respondent that the firmware upgrade tool did not recognize the latest available firmware, and detailed the reasons for the failure. In an internal email from that time, respondent acknowledged that, "if this list is not up to date when you use the check for update button in the [admin console,] the router doesn't find an update and states it is already up to date." Again, in October 2014 and January 2015, additional consumers reported to ASUS that the firmware upgrade tool still did not recognize the latest available firmware.

29.

or risks, and (iii) the availability of srBox(e)6(uTa)pTae thwhore4(ca)4tiori

AIDISK SECURITY MISREPRESENTATIONS (Count 3)

41. As described in Paragraph 14, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its AiDisk feature is a secure means for a consumer to access sensitive personal information.

42. In fact, as described in Paragraphs 14-23 and 30, respondent did not take reasonable steps to ensure that its AiDisk feature is a secure means for a consumer to access sensitive personal information. Therefore, the representation set forth in Paragraph 41 is false or misleading.

FIRMWARE UPGRADE TOOL MISREPRESENTATIONS (Count 4)

43. As described in Paragraph 27, respondent has represented, expressly or by implication, that consumers can rely upon the firmware upgrade tool to indicate accurately whether their router is using the most current firmware.

44. In fact, as described in Paragraphs 28-29, consumers cannot rely upon the firmware upgrade tool to indicate accurately whether their router is using the most current firmware. Therefore, the representation set forth in Paragraph 43 is false or misleading.

UNFAIR SECURITY PRACTICES (Count 5)

45. As set forth in Paragraphs 4-36, respondent has failed to take reasonable steps to secure the software for its routers, which respondent offered to consumers for the purpose of protecting their local networks and accessing sensitive personal information. Respondent’s actions caused or are likely to cause substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair actsubsl-1(ubs)-1(act)-6(i)-6(cTs)-0.9(e)J 4.72 hm2(s) -2.15 Td (44.)Tj /TT2 0/MCID 23 24