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") cameras, and other connected

appliances, against malicious incoming traffic from the internet. Respondent marketed its routers as including security features such as "SPI intrusion detection" and "DoS protection," advertised that its routers could "protect computers from any unauthorized access, hacking, and virus attacks" (*see* Exh. A, p. 1 of 2), and instructed consumers to "enable the [router's] firewall to protect your local network against attacks from hackers" (*see* Exh. A, p. 2 of 2).

5. Consumers set up and control the router's configuration settings, including its security-related settings, through a web-based graphical user interface (the "admin console"). In order to configure these settings, consumers must log in to the admin console with a username and password, which ASUS preset on all of its routers to the default username "admin" and password "admin" (*see* Exh. B). The admin console also provides a tool that ostensibly allows consumers to check whether the router is using the latest available firmware – the software that operates the router.

6. Many of respondent's routers include software features called AiCloud and AiDisk that allow consumers to wirelessly access and share files through their router. Depending on the model, respondent's routers that include these "cloud" features have a list price in the range of $69.99 to $219.99. As of March 2014, respondent had sold over 918,000 of these routers to U.S. consumers.

AICLOUD

7. In August 2012, ASUS introduced and began marketing a feature known as AiCloud on its routers. Respondent publicized AiCloud as a "private personal cloud for selective file sharing" that featured "indefinite storage and increased privacy" (*see* Exh. C, p. 1 of 6). In the following months, ASUS provided software updates for certain older router models to add the AiCloud feature, which respondent touted as "the most complete, accessible, and secure cloud platform" (*see* Exh. C, p. 2 of 6).

8. Described as "your secure space," AiCloud allows consumers to plug a USB storage device, such as an external hard drive, into the router, and then use web and mobile applications to access files on the storage device (*see* Exh. C, p. 3 of 6). For example, a consumer could save documents to the storage device using a desktop computer, and then later access those documents using a laptop, smartphone, or tablet. AiCloud also allows consumers to share specific files with others through a "secure URL," manage shared files, and revoke file access (*see* Exh. C, pp. 3-6 of 6).

Multiple Vulnerabilities

9. The AiCloud web and mobile applications require consumers to log in with the router's username and password (*see* Exh. D). However, the AiCloud web application included multiple vulnerabilities that would allow attackers to gain unauthorized access to consumers' files and router login credentials. In order to exploit these vulnerabilities, an attacker would only need to know the router's IP address – information that, as described in Paragraph 32, is easily discoverable.

10. First, attackers could exploit an authentication bypass vulnerability to access the consumer's AiCloud account without the consumer's login credentials. By sending a specific command, or simply entering a specific URL in a web browser, an attacker could bypass the AiCloud web application's authentication screen and gain unauthorized access to a consumer's files, even if the consumer had not designated any of these files for sharing.

11. Second, attackers could exploit a password disclosure vulnerability in the AiCloud web application to retrieve the consumer's router login credentials in clear, readable text. In addition to providing the attacker with access to the consumer's AiCloud account, attackers could also use these login credentials to gain unauthorized access to the router's configuration settings. For example, if a consumer had enabled the admin console's remote management feature, an attacker could use the login credentials to simply log into the consumer's admin account and modify any of the router's settings, including its firewall and other security settings. Even if this remote management feature was disabled, an attacker could use the credentials in conjunction with other well-known vulnerabilities that affected respondent's routers, such as the cross-site request forgery vulnerabilities described in Paragraphs 24-26, to force unauthorized changes to the router's security settings, placing the consumer's local network at risk.

Failure to Provide Timely Notice

12. Several individuals notified respondent about the AiCloud vulnerabilities in June 2013. Furthermore, in September 2013, a consumer complained to ASUS that his "entire life [was] hacked" due to the AiCloud vulnerabilities, and that he needed to obtain identity theft protection services as a result. Despite knowing about these serious vulnerabilities and their impact on respondent's customers, respondent failed to notify consumers about the vulnerabilities or advise them to take simple steps, such as disabling the AiCloud features, that would have mitigated the vulnerabilities.

13. Between July 2013 and September 2013, ASUS updated the firmware for affected routers in order to correct the AiCloud vulnerabilities. However, it was not until February 2014, eight months after respondent first learned of the vulnerabilities and after the events described in Paragraph 32, that respondent emailed registered customers notifying them that firmware updates addressing these and other security risks were available.

AIDISK

14. ASUS has offered another "cloud" feature on many of its routers called "AiDisk" since as early as 2009. Like AiCloud, AiDisk enables consumers to remotely access files on a USB storage device attached to the router, but does so through a file transfer protocol ("FTP") server. Despite the fact that FTP does not support transit encryption, since at least 2012 respondent has promoted AiDisk as a way to "safely secure and access your treasured data through your router" (*see* Exh. E). In addition to transferring files unencrypted, the AiDisk software included a number of other design flaws that placed consumers' sensitive personal information at risk.

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 FTP server. However, the AiDisk wizard recommended that the consumer choose weak login credentials, such as the preset username "Family" and password "Family" (*see* Exh. F, p. 2 of 2). In the alternative, the consumer could select "admin rights," which would apply the same login credentials for the FTP server that the consumer used to log in to the router's admin console. As described in Paragraphs 11 and 24, however, due to multiple password disclosure vulnerabilities, attackers could access these router login credentials in clear, readable text, undermining the protection provided by these credentials.

19. If a consumer wanted to prevent unauthenticated access through the "USB Application – FTP Share" submenu, the software provided no explanation or guidance as to how the consumer could change the default settings. The consumer would need to know to click on the "Share with account" option (*see* Exh. G, p. 1 of 2), which would allow the consumer to set up login credentials for the AiDisk FTP server. Confusingly, however, the software presented the consumer with a warning that implied that this option would expand, rather than restrict, access to the FTP server: "Enabling share with account enables multiple computers, with different access rights, to access the file resources. Are you sure you want to enable it?" (*see* Exh. G, p. 2 of 2). Through this misleading

warning, respondent discouraged consumers from taking steps that could have prevented unauthenticated access to their sensitive personal information.

Notice of Design Flaws and Failure to Mitigate

20. In June 2013, a security researcher publicly disclosed that, based on his research, more than 15,000 ASUS routers allowed for unauthenticated access to AiDisk FTP servers over the internet. In his public disclosure, the security researcher claimed that he had previously contacted respondent about this and other security issues. In November 2013, the security researcher again contacted respondent, warning that, based on his research, 25,000 ASUS routers now allowed for unauthenticated access to AiDisk FTP servers. The researcher suggested that respondent warn consumers about this risk during the AiDisk set up process. However, ASUS took no action at the time.

21. Two months later, in January 2014, several European media outlets published stories covering the security risks caused by the AiDisk default settings. At that time, a large European retailer requested that respondent update the AiDisk default settings. Although respondent had known about the security risks for months, it was only after this retailer's request that respondent took some steps to protect its customers. In response, ASUS began releasing updated firmware that changed the AiDisk wizard's default setting – for new set-ups – from "limitless access rights" to "limited access rights," and displayed a warning message if consumers selected "limitless access rights" that "any user can access your FTP service without authentication!" However, respondent did not notify consumers about the availability of this firmware update.

22. Moreover, the January 2014 firmware update did not change the insecure default settings for consumers who had already set up AiDisk. Respondent did not notify those consumers that they would need to complete the AiDisk wizard process again in order for the new defaults to apply, or would need to manually change the settings.

23. It was not until February 2014 – following the events described in Paragraph 32 – that respondent sent an email to registered customers notifying them that firmware updates addressing these security risks and other security vulnerabilities were available. Furthermore, it was not until February 21, 2014 that ASUS released a firmware update that would provide some protection to consumers who had previously set up AiDisk. This firmware update forced consumers' routers to turn off unauthenticated access to the AiDisk FTP server.

OTHER VULNERABILITIES

24. ASUS's router firmware and admin console have also been susceptible to a number of other well-known and reasonably foreseeable vulnerabilities – including multiple password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities – that attackers could exploit to gain unauthorized administrative control over consumers' routers.

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. As a result, in many cases, respondent's firmware upgrade tool inaccurately notifies consumers that the "router's current firmware is the latest version" when, in fact, newer firmware with critical security updates is available.

RESPONDENT'S FAILURE TO REASONABLY SECURE ITS ROUTERS AND RELATED "CLOUD" FEATURES

30. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security in the design and maintenance of the software developed for its routers and related "cloud" features. Among other things, respondent failed to:

    a. perform security architecture and design reviews to ensure that the software is designed securely, including failing to:

        i. use readily-available secure protocols when designing features intended to provide consumers with access to their sensitive personal information. For example, respondent designed the AiDisk feature to use FTP rather than a protocol that supports transit encryption;

        ii. implement secure default settings or, at the least, provide sufficient information that would ensure that consumers did not unintentionally expose sensitive personal information;

        iii. prevent consumers from using weak default login credentials to protect critical security functions or sensitive personal information. For example, respondent allowed consumers to retain the weak default login credentials username "admin" and password "admin" for the admin console, and username "Family" and password "Family" for the AiDisk FTP server;

    b. perform reasonable and appropriate code review and testing of the software to verify that access to data is restricted consistent with a user's privacy and security settings;

    c. perform vulnerability and penetration testing of the software, including for well-known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers' sensitive personal information and local networks, such as authentication bypass, clear-text password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities;

    d. implement readily-available, low-cost protections against well-known and reasonably foreseeable vulnerabilities, as described in (c), such as input validation, anti-CSRF tokens, and session time-outs;

    e. maintain an adequate process for receiving and addressing security vulnerability reports from third parties such as security researchers and academics;

    f. perform sufficient analysis of reported vulnerabilities in order to correct or mitigate all reasonably detectable instances of a reported vulnerability, such as those elsewhere in the software or in future releases; and

    g. provide adequate notice to consumers regarding (i) known vulnerabilities or security risks, (ii) steps that consumers could take to mitigate such vulnerabilities

or risks, and (iii) the availability of software updates that would correct or mitigate the vulnerabilities or risks.

THOUSANDS OF ROUTERS COMPROMISED

31. Due to the failures described in Paragraphs 7-30, respondent has subjected its customers to a significant risk that their sensitive personal information and local networks will be subject to unauthorized access.

32. For example, on or before February 1, 2014, a group of hackers used readily available tools to locate the IP addresses of thousands of vulnerable ASUS routers. Exploiting the AiCloud vulnerabilities and AiDisk design flaws, the hackers gained unauthorized access to the attached USB storage devices of thousands of consumers and saved a text file on the storage devices warning these consumers that their routers were compromised: "This is an automated message being sent out to everyone effected [sic]. Your Asus router (and your documents) can be accessed by anyone in the world with an internet connection." The hackers then posted online a list of IP addresses for 12,937 vulnerable ASUS routers as well as the login credentials for 3,131 AiCloud accounts, further exposing these consumers to potential harm.

33. Numerous consumers reported having their routers compromised, based on their discovery of the text-file warning the hackers had saved to their attached USB storage devices. Some complained that a major search engine had indexed the files that the vulnerable routers had exposed, making them easily searchable online. Others claimed to be the victims of related identity theft. For example, one consumer claimed that identity thieves had gained unauthorized access to his USB storage device, which contained his family's sensitive personal information, including login credentials, social security numbers, dates of birth, and tax returns. According to the consumer, in March 2014, identity thieves used this information to make thousands of dollars of fraudulent charges to his financial accounts, requiring him to cancel accounts and place a fraud alert on his credit report. Moreover, the consumer claimed that he had attempted to upgrade his router's firmware on several occasions after he bought the device in December 2013, but that the firmware upgrade tool had erroneously indicated that his router was using the latest available firmware. Given the sensitivity of the stolen personal information, he and his family are at a continued risk of identity theft.

34. Even consumers who did not enable the AiCloud and AiDisk features have been at risk of harm due to numerous vulnerabilities in respondent's router firmware and admin console. As described in Paragraphs 24-26, attackers could exploit these vulnerabilities to gain unauthorized control over a consumer's router and modify its security settings without the consumer's knowledge.

THE IMPACT OF RESPONDENT'S FAILURES ON CONSUMERS

35. As demonstrated by the thousands of compromised ASUS routers, respondent's failure to employ reasonable security practices has subjected consumers to substantial injury. Unauthorized access to sensitive personal information stored on attached USB storage devices, such as financial information, medical information, and private photos and videos, could lead to identity theft, extortion, fraud, or other harm. Unauthorized access and control over the router could also lead to the compromise of other devices on the local network, such as computers, smartphones, IP cameras, or other connected appliances. Finally, such unauthorized access and control could allow an attacker to redirect a consumer seeking, for example, a legitimate financial site to a fraudulent site, where the consumer would unwittingly provide the attacker with sensitive financial information. Consumers had little, if any, reason to know that their sensitive personal information and local networks were at risk.

36. Respondent could have prevented or mitigated these risks through simple, low-cost measures. In several instances, respondent could have prevented consumer harm by simply informing consumers about security risks, and advising them to disable or update vulnerable software. In other cases, respondent could have protected against vulnerabilities by implementing well-known and low-cost protections, such as input validation, anti-CSRF tokens, and session time-outs, during the software design process. Finally, simply preventing consumers from using weak default login credentials would have greatly increased the security of consumers' routers.

ROUTER SECURITY MISREPRESENTATIONS
(Count 1)

37. As described in Paragraph 4, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its routers could protect consumers' local networks from attack.

38. In fact, as described in Paragraphs 11, 24-26, and 30, respondent did not take reasonable steps to ensure that its routers could protect consumers' local networks from attack. Therefore, the representation set forth in Paragraph 37 is false or misleading.

AICLOUD SECURITY MISREPRESENTATIONS
(Count 2)

39. As described in Paragraphs 7-8, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its AiCloud feature is a secure means for a consumer to access sensitive personal information.

40. In fact, as described in Paragraphs 9-13 and 30, respondent did not take reasonable steps to ensure that its AiCloud feature is a secure means for a consumer to access sensitive personal information. Therefore, the representation set forth in Paragraph 39 is false or misleading.

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 act or practice.

46. The acts and practices of respondent 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, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this eighteenth day of July, 2016, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary