

Complaint

IN THE MATTER OF

ASUSTEK COMPUTER, INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4587; File No. 142 3156
Complaint, July 18, 2016 – Decision, July 18, 2016

This consent order addresses ASUSTeK Computer, Inc.'s marketing of its routers, and related software and services, intended for consumer use. The complaint alleges that despite respondent's representations, ASUS 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. The consent order requires ASUS to establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing covered devices; and (2) protect the privacy, security, confidentiality, and integrity of covered information.

Participants

For the *Commission*: Jarad Brown, and Nithan Sannappa.

For the *Respondent*: Law Offices of David A. Balto.

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.

Complaint

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.

Complaint

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.

Complaint

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.

Complaint

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

Complaint

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

Complaint

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.

Complaint

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

Complaint

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

Complaint

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;

Complaint

- 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

Complaint

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,

Complaint

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.

Complaint

**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.

Complaint

Therefore, the representation set forth in Paragraph 43 is false or misleading.

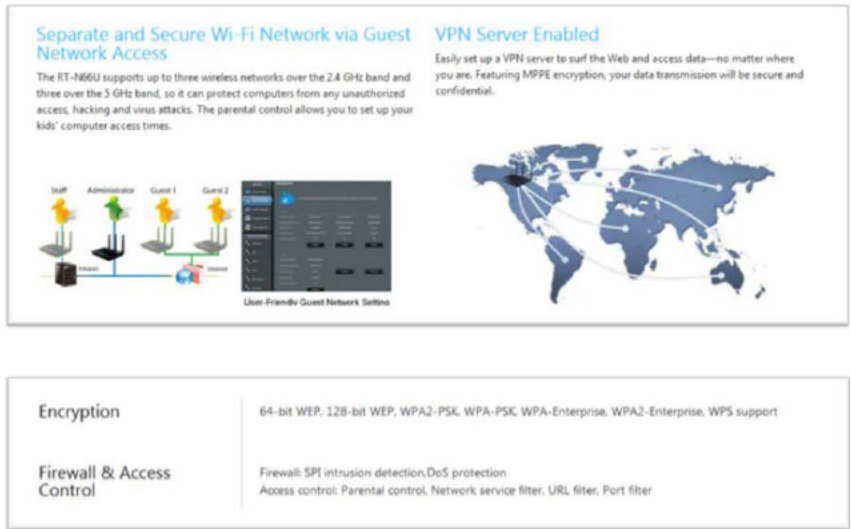
**UNFAIR SECURITY PRACTICES
(Count 5)**

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.

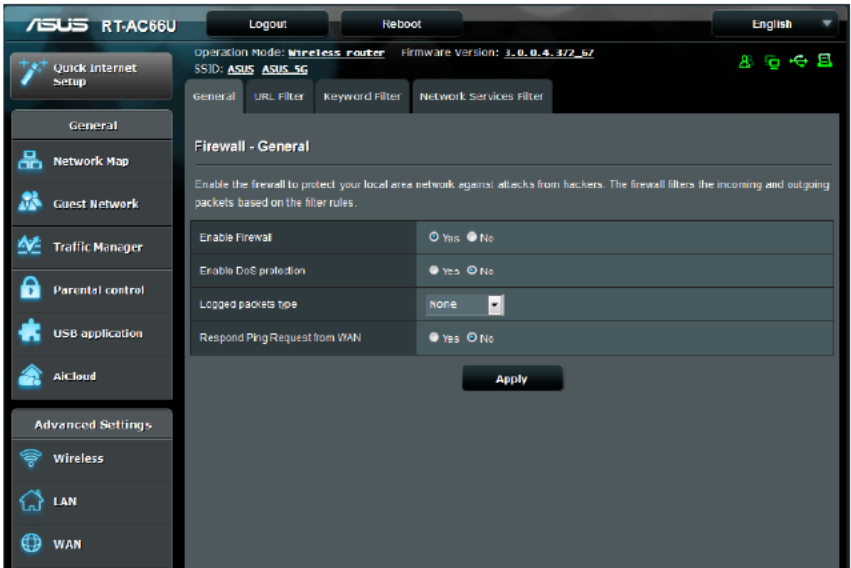
46. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

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

By the Commission.



Exh. A, p. 1 of 2, Examples of Security Features Respondent Marketed in Router Product Descriptions

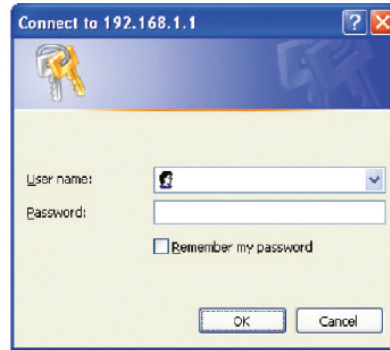


Exh. A, p. 2 of 2, Respondent's Router Security Representation

Complaint

Exhibit B

1. On your web browser such as Internet Explorer, Firefox, Safari, or Google Chrome, manually key in the wireless router's default IP address: **192.168.1.1**
2. On the login page, key in the default user name (**admin**) and password (**admin**).



Exh. B, Respondent's Login Instructions

Complaint

Exhibit C

ASUS Introduces AiCloud and a Range of New Innovations at IFA

Enriching users' digital lives with the latest technologies

2012/08/29

ASUS, a global leader in the new digital era, today announces a number of new products that are designed to work together to enrich users' digital lives with the latest technologies. ASUS AiCloud combines a cutting-edge 802.11ac Wi-Fi router with easy-to-use services that allow anyone to create their own personal cloud storage; while two new Design MX monitors deliver incredible visuals in a stunningly slim and elegant design.

Gamers have not been overlooked either with the introduction of the powerful ASUS ROG TYTAN CG8890 gaming desktop; while business users can deliver crystal-clear presentations with the compact B1 Portable LED Projector designed to maximize ease-of-use and mobility. In addition, the Zen-inspired ASUS SDRW-080S-U External DVD Writer makes a perfect companion for the ZENBOOK™.

ASUS AiCloud – make an incredible connection

ASUS AiCloud brings the convenience of cloud-based storage to everyone with a combination of easy-to-use technology and services, as well as indefinite storage and increased privacy. Smart Access lets users keep all their data on their home network or online storage facility easily accessible from anything from a smartphone to a PC, as long as they have an internet connection. It allows any networked computer to be incorporated into a private personal cloud for selective file sharing over the internet, using any compatible Windows, Mac and Linux device. Files can be easily shared through a simple web link.

Cloud Disk gives users access to an always-on data and media library by connecting a USB storage drive to an ASUS router like the RT-AC66U to act as a cloud services hub. This gives users their own media server on everything from Android or iOS-based smartphones or tablets to notebooks and no longer need to store space-hungry music and movie collections locally.

ASUS Smart Sync makes it easy to synchronise data on local storage devices with an ASUS WebStorage account. Synchronisation is automatic and takes place in real time to ensure that files are always up to date.

Exh. C, p. 1 of 6, Respondent's AiCloud Press Release

FAST Networking Solutions
FAST · EASY · STABLE Networks & Wireless Products E-News, Apr-May, 2013

RP-N53 RT-N14U **Product Updates**

RT-N56U/DSL-N55U supports ASUSWRT & AiCloud

AiCloud: Sync, share, and stream everywhere

ASUS AiCloud works with ASUS routers to offer the most complete, accessible, and secure cloud platform. It's a free app for iOS and Android devices, and allows you to easily sync, share, stream, and access all your content from any location. It creates your own private cloud server at home, and connects it seamlessly with the public cloud. Sharing is easier than ever with confidential links, which can be sent via email, SMS, and more. For the most intuitive and flexible cloud access from almost any device and location, ASUS AiCloud is your launch point.

ASUSWRT: Intuitive network setup and control

ASUSWRT moves network setup and settings easy and accessible for a better experience. Optimize your connection with one click QoS bandwidth prioritization, network mapping, printer sharing, and parental controls – all through one graphical interface.

Stream media using AiCloud Share files using AiCloud

Exh. C, p. 2 of 6, Respondent's AiCloud Product Update News Release

Complaint

Do more with your AiCloud



Remotely access home PCs

With AiCloud, easily access and share your files from any connected PC. Now, you'll always have your files on hand wherever you go.



Sync with WebStorage and other AiCloud accounts

AiCloud quickly syncs all your devices to your ASUS WebStorage account with instant file version updates, plus share files with other AiCloud accounts* easily.



Share files with a simple link

Instantly and easily share videos, music, and documents to others with a simple, shareable link with AiCloud.



Stream video and audio from your home

AiCloud lets you easily stream videos, music, and movies from an AiCloud media library straight to your smartphone or notebook, saving you storage space and time with convenience.



Access files even with your computers in sleep mode

See every device with its connection status, and even wake up and access computers connected to ASUS routers via wired LAN remotely.



Unlimited expansion

Connect as many devices and online storage services* as you want, together with AiCloud for ample storage space for all your contents.



Your secure space

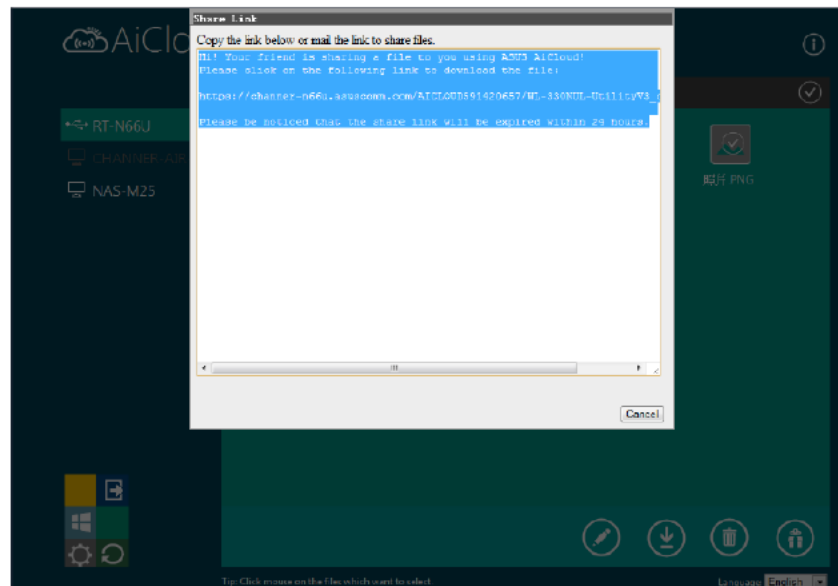
Instantly and easily share videos, music, and documents to others with a simple, shareable link with AiCloud.



Download now

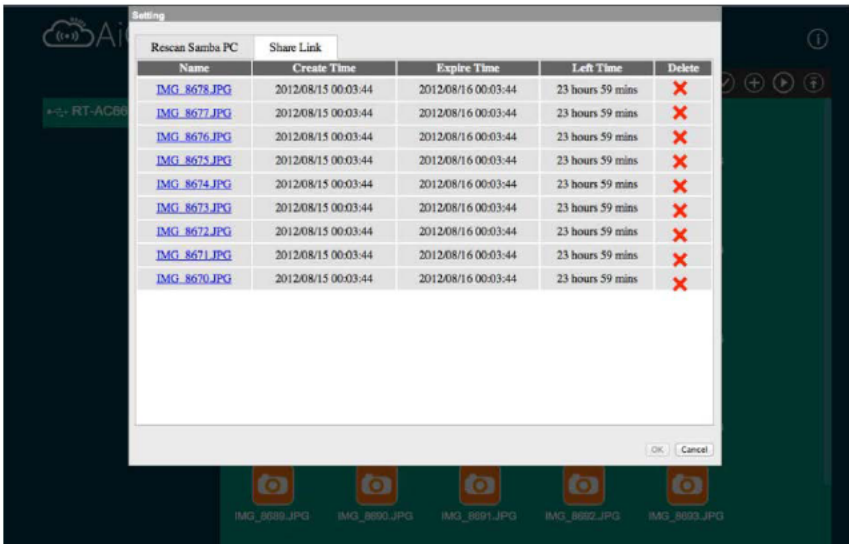
ASUS AiCloud App is now available on App Store and Google Play. You can download it now, and enjoy Cloud Disk, Smart Sync and Smart Access.

Exh. C, p. 3 of 6, Respondent's AiCloud Website: "Your secure space"



Exh. C, p. 4 of 6, AiCloud Web Application Share Link

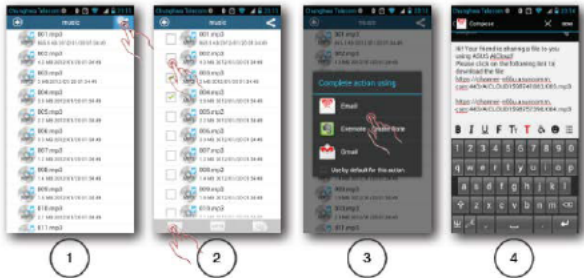
Complaint



Exh. C, p. 5 of 6, AiCloud Web Application Share Link Manager

Sharing the file to friend with
secure URL by App

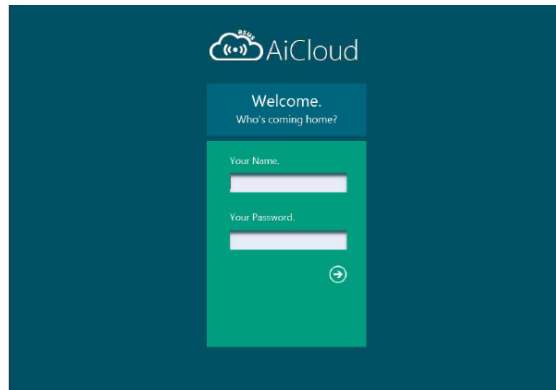
Cloud Disk offers you an easy way to share files with friends. Simply open AiCloud, then choose the specific files you want to share. Cloud Disk creates short HTTPS links for those files. You can then can select a way to share (via email, SMS, or copying links to other popular communication applications) these links with other people instantly.



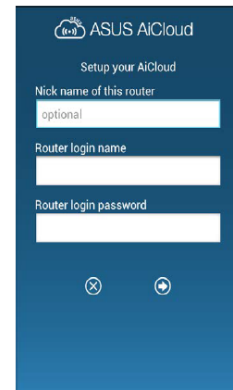
- Steps:**
- (1) Tap the function icon at the upper right corner.
 - (2) Tap the check box in front of the file you wan to share, then click the button corresponding to the way you want to share the file's URL.
 - (3) Click email: you can send URLs by Bluetooth, Evernote, and normal email apps such as Gmail.
 - (4) The HTTPS file's URL is automatically added in the mail body, but you can edit mail contents before sending.

Exh. C, p. 6 of 6, AiCloud User Manual Explaining Mobile Sharing Options

Complaint

Exhibit D

Web Application



Mobile Application

Exh. D, AiCloud Web Application and Mobile Application Login Screens

Complaint

Exhibit E**The Ultra Versatile Download Master**[View larger](#)

The RT-N56U router sets itself apart from ordinary routers by offering BitTorrent and FTP server functionality.

BitTorrent

Share your movies, music, games, and other files. The included Download Master application utilizes the BitTorrent P2P protocol to download and seed Torrents to and from the connected USB storage device. What's more, you can shut off your PC after setting up a torrent file to continue the download, PC-free. Download Master also lets you customize how you choose to share with custom bandwidth allocation when seeding.

FTP

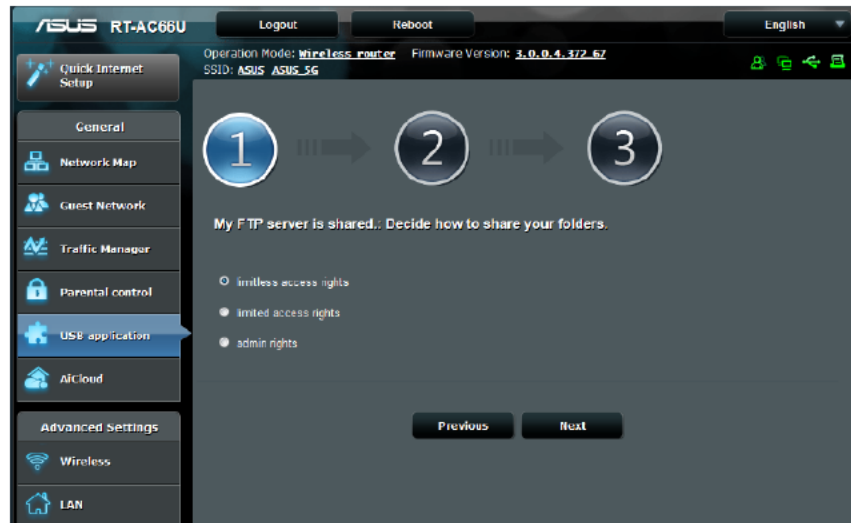
Create your own personal FTP Server with ASUS AiDisk located within the EZ UI, and upload or download files from the connected USB storage device to any Internet-accessible PCs. Perfect when you forget documents at home or when sharing large files, FTP access grants you the ability to safely secure and access your treasured

data through your router. This feature can also work without having to leave your PC on.

Exh. E, Respondent's Description of AiDisk on Retailer Website

Complaint

Exhibit F



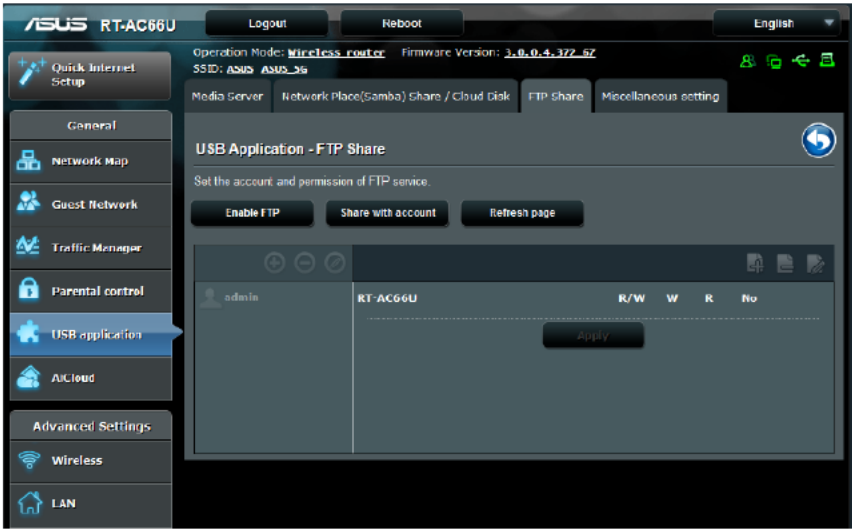
Exh. F, p. 1 of 2, AiDisk Wizard “limitless access rights” Default Setting



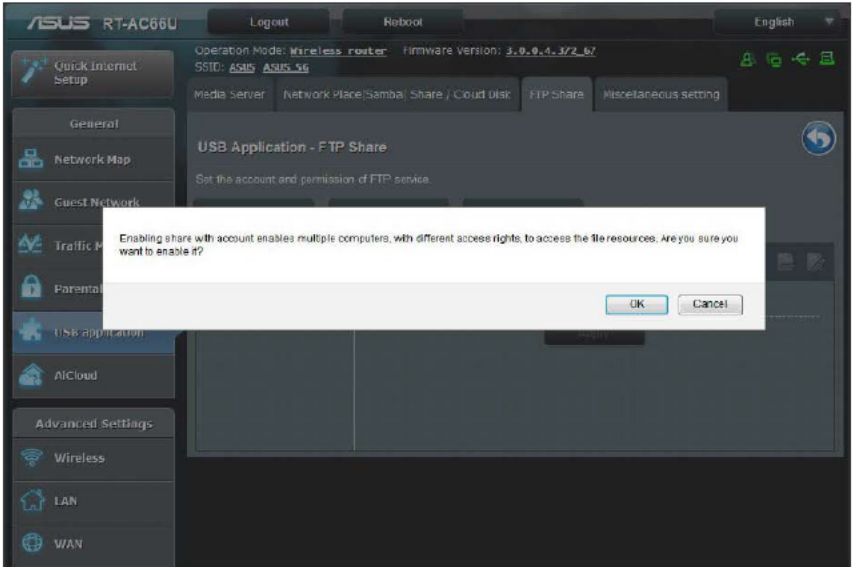
Exh. F, p. 2 of 2, Weak Recommended Login Credentials

Complaint

Exhibit G

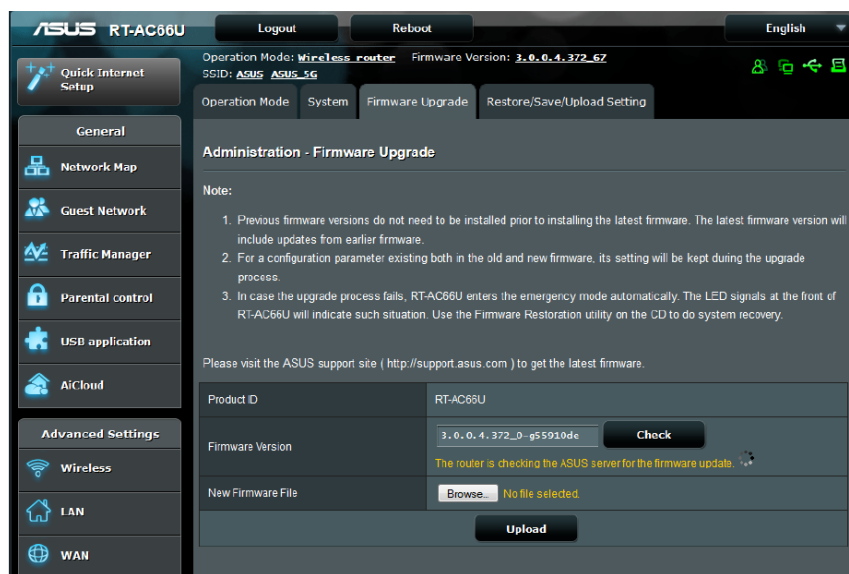


Exh. G, p. 1 of 2, “Enable FTP” and “Share with account” Options



Exh. G, p. 2 of 2, “Share with account” Warning

Decision and Order

Exhibit H

Exh. H, Firmware Upgrade Tool

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named above in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violation of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for

Decision and Order

purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days, and duly considered the comments filed thereafter by interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

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 Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

- A. Unless otherwise specified, "respondent" shall mean ASUSTeK Computer, Inc., corporation, and its subsidiaries and divisions in the United States, and successors and assigns.
- B. "Clear(ly) and conspicuous(ly)" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

Decision and Order

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication, even if the representation requiring the disclosure is made in only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers.
 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
- C. “Commerce” shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or

Decision and Order

between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

- D. “Covered Device” shall mean (a) any router, or device for which the primary purpose is connecting other client devices to a network, developed by respondent, directly or indirectly, that is marketed to consumers in the United States and (b) the software used to access, operate, manage, or configure such router or other device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or provided by respondent, directly or indirectly, for use with, or as compatible with, the router or other device.
- E. “Covered Information” shall mean any individually-identifiable information from or about an individual consumer collected by respondent through a Covered Device or input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to (a) a first and last name; (b) a home or other physical address; (c) an email address or other online contact information; (d) a telephone number; (e) a Social Security number; (f) financial information; (g) an authentication credential, such as a username or password; (h) photo, video, or audio files; (i) the contents of any communication, the names of any websites sought, or the information entered into any website.
- F. “Default Settings” shall mean any configuration option on a Covered Device that respondent preselects, presets, or prefills for the consumer.
- G. “Software Update” shall mean any update designed to address a Security Flaw.

Decision and Order

- H. “Security Flaw” is a software vulnerability or design flaw in a Covered Device that creates a material risk of (a) unauthorized access to or modification of any Covered Device, (b) the unintentional exposure by a consumer of Covered Information, or (c) the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of Covered Information.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, in or affecting commerce, must not misrepresent in any manner, expressly or by implication:

- A. The extent to which respondent or its products or services maintain and protect:
1. The security of any Covered Device;
 2. The security, privacy, confidentiality, or integrity of any Covered Information;
- B. The extent to which a consumer can use a Covered Device to secure a network; and
- C. The extent to which a Covered Device is using up-to-date software.

II.

IT IS FURTHER ORDERED that respondent must, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing Covered Devices, and (2) protect the privacy, security, confidentiality, and integrity of Covered Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards

Decision and Order

appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information, including:

- A. The designation of an employee or employees to coordinate and be accountable for the security program;
- B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or unauthorized modification of a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;
- C. The identification of material internal and external risks to the privacy, security, confidentiality, and integrity of Covered Information that could result in the unintentional exposure of such information by consumers or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;
- D. At a minimum, the risk assessments required by Subparts B and C must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing, including for Default Settings; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;
- E. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, such as (1) vulnerability and penetration testing; (2) security

Decision and Order

architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Devices and Covered Information is restricted consistent with a user's security settings;

- F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this order; and
- H. The evaluation and adjustment of respondent's security program in light of the results of the testing and monitoring required by Subpart F, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent must obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments must be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Internet-accessible consumer-grade devices; or a similarly qualified person or organization

Decision and Order

approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment must:

- A. Set forth the specific controls and procedures that respondent has implemented and maintained during the reporting period;
- B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information;
- C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Devices and the privacy, security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment must be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent must provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments must be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent

Decision and Order

Assessments requested, must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

IV.

IT IS FURTHER ORDERED that respondent must:

- A. Notify consumers, Clearly and Conspicuously, when a Software Update is available, or when respondent is aware of reasonable steps that a consumer could take to mitigate a Security Flaw. The notice must explain how to install the Software Update, or otherwise mitigate the Security Flaw, and the risks to the consumer's Covered Device or Covered Information if the consumer chooses not to install the available Software Update or take the recommended steps to mitigate the Security Flaw. Notice must be provided through at least each of the following means:
 - 1. Posting of a Clear and Conspicuous notice on at least the primary, consumer-facing website of respondent and, to the extent feasible, on the user interface of any Covered Device that is affected;
 - 2. Directly informing consumers who register, or who have registered, a Covered Device with respondent, by email, text message, push notification, or another similar method of providing notifications directly to consumers; and
 - 3. Informing consumers who contact respondent to complain or inquire about any aspect of the Covered Device they have purchased.
- B. Provide consumers with an opportunity to register an email address, phone number, device, or other information during the initial setup or configuration of

Decision and Order

a Covered Device, in order to receive the security notifications required by this Part. The consumer's registration of such information must not be dependent upon or defaulted to an agreement to receive non-security related notifications or any other communications, such as advertising. Notwithstanding this requirement, respondent may provide an option for consumers to opt-out of receiving such security-related notifications.

V.

IT IS FURTHER ORDERED that respondent must maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

- A. For a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Part III of this order, for the compliance period covered by such Assessment;
- B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:
 - 1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation;

Decision and Order

2. All notifications required by Part IV of this order;
and
3. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent must deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent must deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery must be at least ten (10) days prior to the change in structure.

VII.

IT IS FURTHER ORDERED that respondent must notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent must notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of

Decision and Order

Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

VIII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, must file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it must submit additional true and accurate written reports.

IX.

This order will terminate on July 18, 2036, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in fewer than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing

Analysis to Aid Public Comment

such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to ASUSTeK Computer, Inc. (“ASUS”).

The proposed consent order has 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 agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

ASUS is a hardware manufacturer that, among other things, sells routers, and related software and services, intended for consumer use. 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. ASUS marketed its routers as including security features such as “intrusion detection,” and instructed consumers to “enable the [router’s] firewall to protect your local network against attacks from hackers.”

Many of ASUS’s routers also include “cloud” software features called AiCloud and AiDisk that allow consumers to attach a USB storage device to their router and then wirelessly

Analysis to Aid Public Comment

access and share files. ASUS publicized AiCloud as a “private personal cloud for selective file sharing” that featured “indefinite storage and increased privacy” and described the feature as “the most complete, accessible, and secure cloud platform.” Similarly, ASUS promoted AiDisk as a way to “safely secure and access your treasured data through your router.”

The Commission’s complaint alleges that, despite these representations, ASUS 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. The complaint challenges these failures as both deceptive and unfair. Among other things, the complaint alleges that ASUS 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, ASUS 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. For example, respondent allowed consumers to retain weak default login credentials to protect critical functions, such as 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

Analysis to Aid Public Comment

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.

The Complaint further alleges that, due to these failures, ASUS has subjected its customers to a significant risk that their sensitive personal information and local networks will be subject to unauthorized access. For example, on or before February 1, 2014, a group of hackers exploited vulnerabilities and design flaws in ASUS's routers to gain unauthorized access to thousands of consumers' USB storage devices. Numerous consumers reported having their routers compromised, and some complained

Analysis to Aid Public Comment

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, including a consumer who claimed identity thieves had gained unauthorized access to his USB storage device, which contained his family's sensitive personal information, such as login credentials, social security numbers, dates of birth, and tax returns. According to the consumer, the 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. In addition, in April 2015, a malware researcher discovered a large-scale, active 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.

The proposed consent order contains provisions designed to prevent ASUS from engaging in the future in practices similar to those alleged in the complaint. Part I of the proposed consent order prohibits ASUS from misrepresenting: (1) the extent to which it maintains and protects the security of any covered device (including routers), or the security, privacy, confidentiality, or integrity of any covered information; (2) the extent to which a consumer can use a covered device to secure a network; and (3) the extent to which a covered device is using up-to-date software.

Part II of the proposed consent order requires ASUS to establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing covered devices; and (2) protect the privacy, security, confidentiality, and integrity of covered information. The security program must contain administrative, technical, and physical safeguards appropriate to ASUS's size and complexity, nature and scope of its activities, and the sensitivity of the covered device's function or the sensitivity of the covered information. Specifically, the proposed order requires ASUS to:

- a. designate an employee or employees to coordinate and be accountable for the information security program;

Analysis to Aid Public Comment

- b. identify material internal and external risks to the security of covered devices that could result in unauthorized access to or unauthorized modification of a covered device, and assess the sufficiency of any safeguards in place to control these risks;
- c. identify material internal and external risks to the privacy, security, confidentiality, and integrity of covered information that could result in the unintentional exposure of such information by consumers or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;
- d. consider risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing, including for default settings; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;
- e. design and implement reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- f. develop and use reasonable steps to select and retain service providers capable of maintaining security practices consistent with the order, and require service providers by contract to implement and maintain appropriate safeguards; and
- g. evaluate and adjust its information security program in light of the results of testing and monitoring, any

Analysis to Aid Public Comment

material changes to ASUS's operations or business arrangement, or any other circumstances that it knows or has reason to know may have a material impact on its security program.

Part III of the proposed consent order requires ASUS to obtain, within the first one hundred eighty (180) days after service of the order and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed consent order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered devices and the privacy, security, confidentiality, and integrity of covered information is protected.

Part IV of the proposed consent order requires ASUS to provide clear and conspicuous notice to consumers when a software update for a covered device that addresses a security flaw is available or when ASUS is aware of reasonable steps that a consumer could take to mitigate a security flaw in a covered device. In addition to posting notice on its website and informing consumers that contact the company, ASUS must provide security-related notifications directly to consumers. For this purpose, ASUS must provide consumers with an opportunity to register an email address, phone number, device, or other information during the initial setup or configuration of a covered device.

Parts V through IX of the proposed consent order are reporting and compliance provisions. Part V requires ASUS to retain documents relating to its compliance with the order. The order requires that materials relied upon to prepare the assessments required by Part III be retained for a three-year period, and that all other documents related to compliance with the order be retained for a five-year period. Part VI requires dissemination of the order now and in the future to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees,

Analysis to Aid Public Comment

agents, and representatives having supervisory responsibilities relating to the subject matter of the order. Part VII ensures notification to the FTC of changes in corporate status. Part VIII mandates that ASUS submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part IX is a provision “sunsetting” the order after (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed consent order. It is not intended to constitute an official interpretation of the proposed complaint or consent order or to modify the consent order’s terms in any way.

Complaint

IN THE MATTER OF

LABMD, INC.COMPLAINT, OPINION OF THE COMMISSION AND FINAL ORDER IN
REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE
FEDERAL TRADE COMMISSION ACT

Docket No. 9357; File No. 102 3099
Complaint, August 28, 2013 – Order, July 28, 2016

This case addresses LabMD, Inc.’s alleged failure to protect the sensitive personal information, including medical information, of consumers whose physicians had entrusted that information to the company. The complaint alleges that LabMD failed to implement reasonable security measures to protect the sensitive consumer information on its computer network and therefore that its data security practices were unfair under Section 5 of the Federal Trade Commission Act. In his Initial Decision, 160 F.T.C. 1190 (2015), the Administrative Law Judge dismissed the Complaint following an administrative trial, holding that Complaint Counsel had not shown that LabMD’s data security practices either caused or were likely to cause substantial injury. The Commission reversed the ALJ’s decision and ordered LabMD to notify affected consumers, establish a comprehensive information security program reasonably designed to protect the security and confidentiality of the personal consumer information in its possession, and obtain independent assessments regarding its implementation of the program.

Participants

For the *Commission*: Megan Cox, Maggie Lassack, Ryan Mehm, Laura Riposo VanDruff, Alain Sheer, and Ruth Yodaiken.

For the *Respondent*: Stephen Fusco, Fusco & Associates, LLC; Charles C. Murphy, Jr., Vaughan & Murphy; and Amber Abassi. *Cause of Action*.

COMPLAINT

The Federal Trade Commission (“Commission”), having reason to believe that LabMD, Inc. (“LabMD” or “respondent”), a corporation, 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: