Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of ASUSTeK Computer, Inc.,
File No. 142 3156

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 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 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 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;

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 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, 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.