FTC Announces Settlement with ASUS over Insecure Routers and Cloud Services

Alysa Z. Hutnik

February 24, 2016

Yesterday, the FTC announced that it had entered into a settlement agreement with Taiwan-based computer hardware manufacturer ASUSTeK Computer Inc., resolving allegations that the company failed to take reasonable steps to secure its routers and cloud services. Such failure, the FTC claims, constitutes an unfair practice, in violation of Section 5 of the FTC Act.

Additionally, the complaint alleges that ASUS misrepresented the security of its routers to consumers, through claims such as "the most complete, accessible, and secure cloud platform" and "safely secure and access your router." In reality, however, multiple vulnerabilities – including the failure to encrypt consumer files in transit – allegedly allowed unauthorized access to consumer files and router login credentials. According to the FTC, ASUS was aware of these vulnerabilities as early as June 2013, but did not notify consumers of firmware updates until February 2014.

Under the terms of the settlement, ASUS has agreed to clearly and conspicuously notify consumers of available software updates, and to implement a comprehensive security program that (1) addresses security risks related to the development and management of its routers and router software, and (2) protects the privacy, security, confidentiality, and integrity of customer personal information transmitted via the routers. Specifically, the program must:

- Designate an employee to coordinate and be accountable for the program;
- Identify material internal and external risks to security, and assess the sufficiency of any safeguards in place to control those risks;
- Design and implement reasonable safeguards to control the identified risks, including through reasonable and appropriate software security testing techniques;
- Regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- Develop and use reasonable steps to select and retain service providers capable of maintaining security practices consistent with the order, and require by contract that service providers implement and maintain appropriate safeguards consistent with the order; and
- Evaluate and adjust the program in light of the results of testing and monitoring, any material changes to ASUS's operations or business arrangements, or any other circumstances that may have a material impact on the effectiveness of the program.

Importantly, ASUS's compliance with this requirement for a comprehensive security program is

subject to independent audits for the next 20 years. This settlement serves as yet another reminder that the FTC remains focused on cyber security, and that it is important for all businesses that handle or have access to customer information to ensure that they have implemented reasonable security practices. Failure to do so could result in a lengthy and expensive investigation, followed by a 20-year order.