Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of TRENDnet, Inc., File No. 1223090

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order applicable to TRENDnet, Inc. ("TRENDnet").

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.

TRENDnet is a California corporation that among other things, sells networking devices, such as routers, modems, and Internet Protocol ("IP") security cameras that allow users to conduct remote surveillance of their homes and businesses via the Internet. In many instances, TRENDnet markets its IP cameras under the trade name "SecurView," and tells consumers they may use the cameras to monitor "babies at home, patients in the hospital, offices and banks, and more." By default, these IP cameras are subject to security settings, such as a requirement to enter a user name and password ("login credentials") in order to access the live video and audio feeds ("live feeds") over the Internet. On approximately January 10, 2012, a hacker discovered a flaw in the IP cameras that allowed access to these live feeds without entering login credentials, resulting in hundreds of previously private live feeds being made public.

The Commission's complaint alleges that TRENDnet violated Section 5(a) of the FTC Act by falsely representing that it had taken reasonable steps to ensure that its IP cameras and mobile apps are a secure means to monitor private areas of a consumer's home or workplace. The complaint also alleges that TRENDnet misrepresented that it had taken reasonable steps to ensure that a user's security settings on its devices would be honored. Finally, the Commission's complaint alleges that TRENDnet engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to personal information, namely the live feeds from the IP cameras. Among other things, TRENDnet:

(1) transmitted user login credentials in clear, readable text over the Internet, despite the existence of free code libraries (i.e., repositories of programming language that can be integrated by third parties), publicly available since at least 2008, that would have enabled respondent to secure such transmissions;

(2) stored user login credentials in clear, readable text on a user's mobile device, despite the existence of free software, publicly available since 2008, that would have enabled respondent to secure such stored credentials;

(3) failed to implement a process to actively monitor security vulnerability reports from third-party researchers, academics, or other members of the public, despite the existence of free tools to conduct such monitoring, thereby delaying the opportunity to correct discovered vulnerabilities or respond to incidents;

(4) failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers to install, operate, and access its IP cameras. Among other things, TRENDnet, either directly or through its service providers, failed to:

a) perform security review and testing of the software at key points, such as upon the release of the IP camera or upon the release of software to install, operate, or access the IP camera, including measures such as:

i. a security architecture review to evaluate the effectiveness of the software's security infrastructure;

ii. vulnerability and penetration testing of the software, such as by inputting invalid, unanticipated, or random data to the software;

iii. 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; and

b) implement reasonable guidance or training for any employees responsible for the testing, designing, and reviewing the security of its IP cameras and related software.

The complaint further alleges that, due to these failures, TRENDnet subjected users to a significant risk that their live feeds would be compromised, thereby causing significant injury to consumers. Moreover, the complaint alleges that affected consumers include not only those consumers who maintained login credentials for their cameras, but also unwitting third parties who were present in locations under surveillance by the cameras. The exposure of personal information through TRENDnet's IP cameras increases the likelihood that consumers or their property will be targeted for theft or other criminal activity, increases the likelihood that consumers' personal activities or the activities of their young children or other family members will be observed and recorded by strangers over the Internet, impairs consumers' peaceful enjoyment of their homes, increases consumers' susceptibility to physical tracking or stalking, and reduces consumers' ability to control the dissemination of personal or proprietary information (e.g., intimate video and audio streams or images from business properties). Indeed, consumers had little, if any, reason to know that their information was at risk, particularly if those consumers maintained login credentials for their cameras or were merely unwitting third parties present in locations where the cameras were used.

The proposed order contains provisions designed to prevent TRENDnet from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits TRENDnet from misrepresenting (1) the extent to which TRENDnet or its products or services maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of any covered information; and (2) the extent to which a consumer can control the security of any covered information input into, stored on, captured with, accessed, or transmitted by a covered device.

Part II of the proposed order requires TRENDnet to establish and implement, and thereafter maintain, a comprehensive security program to (1) address security risks that could result in unauthorized access to or use of the functions of covered devices, and (2) protect the security, confidentiality, and integrity of covered information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a covered device. The security program must contain administrative, technical, and physical safeguards appropriate to TRENDnet's size and complexity, nature and scope of its activities, and the sensitivity of the information collected from or about consumers. Specifically, the proposed order requires TRENDnet to:

(1) designate an employee or employees to coordinate and be accountable for the security program;

(2) identify material internal and external risks to the security of covered devices that could result in unauthorized access to or use of covered device functionality, and assess the sufficiency of any safeguards in place to control these risks;

(3) identify material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in TRENDnet's possession or is input into, stored on, captured with, accessed, or transmitted through a covered device, and assess the sufficiency of any safeguards in place to control these risks;

(4) consider risks in each area of relevant operation, including but not limited to (a) employee training and management; (b) product design, development and research; (c) secure software design, development, and testing; and (d) review, assessment, and response to third-party security vulnerability reports;

(5) design and implement reasonable safeguards to control the risks identified through risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (a) vulnerability and penetration testing; (b) security architecture reviews; (c) code reviews; and (d) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to covered information is restricted consistent with a user's security settings;

(6) regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

(7) 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 establish and implement, and thereafter maintain, appropriate safeguards; and

(8) evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to TRENDnet'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 order requires TRENDnet 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 order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered device functionality and the security, confidentiality, and integrity of covered information is protected.

Part IV of the proposed order requires TRENDnet to notify consumers whose cameras were affected by the breach that their IP cameras had a flaw that allowed third parties to access their live feeds without inputting login credentials; and provide instructions to such consumers on how to remove this flaw. In addition, TRENDnet must provide prompt and free support with clear and prominent contact information to help consumers update and/or uninstall their IP cameras. TRENDnet must provide this support via a toll-free, telephonic number and via electronic mail for two (2) years.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires TRENDnet to retain documents relating to its compliance with the order for a five-year period. Part VI requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with 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 TRENDnet submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part IX is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

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