122 3090

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. C-4426**
TRENDNET, INC.,	)	
a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that TRENDnet, Inc., a corporation, has violated the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent TRENDnet, Inc. ("TRENDnet" or "respondent") is a California corporation with its principal office or place of business at 20675 Manhattan Place, Torrance, California 90501.

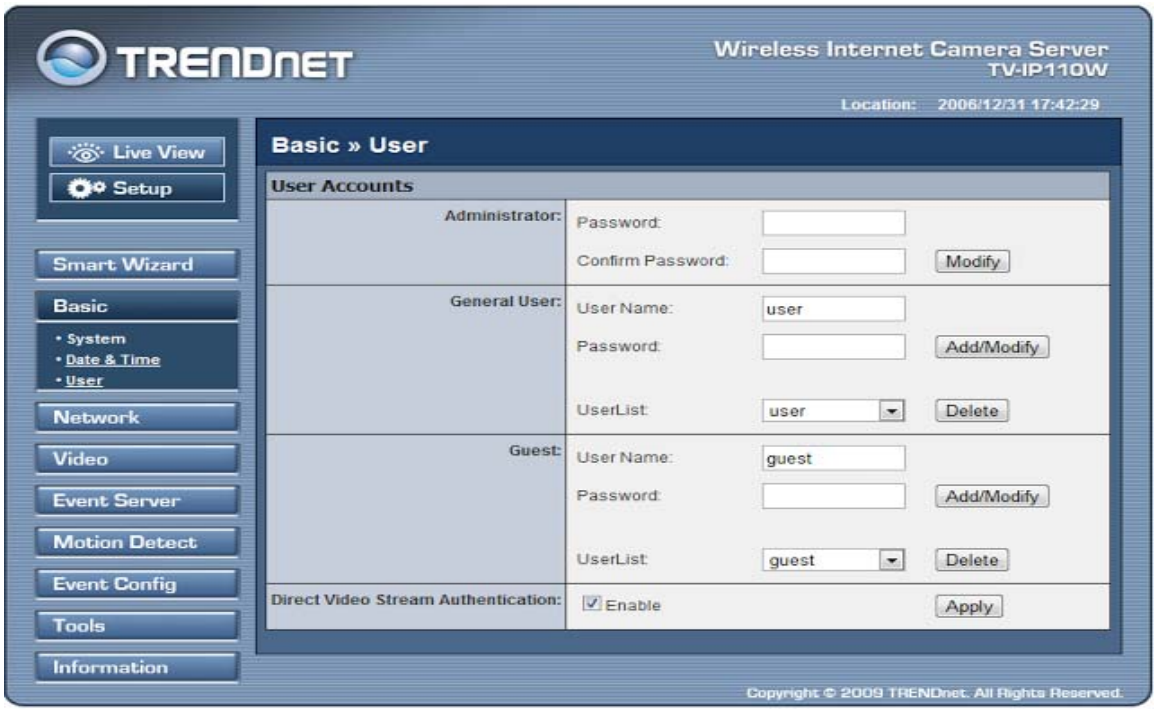
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent is a retailer that among other things, sells networking devices, such as routers, modems, and Internet Protocol ("IP") cameras, to home users and to small- and medium-sized businesses. In 2010, respondent had approximately $64 million in total revenue, and obtained approximately $6.3 million of this amount from the sale of IP cameras. In 2011, respondent had approximately $66 million in total revenue and obtained approximately $5.28 million of this amount from the sale of its IP cameras. Similarly, in 2012, the company had approximately $62 million in total revenue and obtained approximately $7.4 million of this amount from the sale of IP cameras. During this time, the company had approximately 80 employees.

4. Respondent offers its IP cameras for consumers to conduct security monitoring of their homes or businesses, by accessing live video and audio feeds ("live feeds") from their cameras over the Internet. In many instances, these cameras are marketed under the trade name "SecurView." According to respondent, the IP cameras may be used to monitor "babies at home, patients in the hospital, offices and banks, and more."

5. By default, respondent has required users to enter a user name and password ("login credentials"), in order to access the live feeds from their cameras over the Internet. In addition, since at least February 2010, respondent has provided users with a Direct Video Stream Authentication setting ("DVSA setting"), the same as or similar to the one depicted below. The DVSA setting allows users to turn off the login credentials requirement for their cameras, so that they can make their live feeds public. To remove the login credentials requirement, a user would uncheck the box next to the word "Enable," and then "Apply" this selection.



6. Respondent also has provided software applications that enable users to access their live feeds from a mobile device ("mobile apps"), including its SecurView Mobile Android app, which respondent launched in January 2011, and its SecurView PRO Android app, which respondent launched in October 2012. Both apps require that a user enter login credentials the first time that the user employs the app on a particular mobile device. Both apps then store the user's login credentials on that mobile device, so that the user will not be required to enter login credentials on that device in the future.

RESPONDENT'S STATEMENTS TO CONSUMERS

7. From at least January 1, 2010, until the present, in many instances, in marketing or offering for sale its IP cameras, respondent has:

    a. used the trade name SecurView:

        i. in the product names and descriptions displayed on the cameras' packaging (*see, e.g.*, Exhs. A-J);

        ii. in product descriptions on respondent's website and in other advertisements (*see, e.g.*, Exhs. K-L); and

        iii. in the name of its SecurView Mobile and SecurView PRO Android apps, described in **Paragraph 6**.

    b. described the IP cameras as "secure" or suitable for maintaining security, including through:

        i. a sticker affixed to the cameras' packaging, the same as or similar to the one depicted below, which displays a lock icon and the word "security" (*see, e.g.*, Exhs. B, D, F-H, J);

        ii. a statement on the cameras' packaging that it may be used to "secure," or "protect" a user's home, family, property, or business (*see, e.g.*, Exhs. A, B, I); and

        iii. product descriptions on respondent's website and in other advertisements (*see, e.g.*, Exhs. K-M);

    c. provided an authentication feature, which requires users to enter login credentials before accessing the live feeds from their IP cameras over the Internet; and

d. provided the DVSA setting, described in **Paragraph 5**, which purports to allow users to choose whether login credentials will be required to access the live feeds from their IP cameras over the Internet.

RESPONDENT'S FAILURE TO REASONABLY SECURE ITS IP CAMERAS AGAINST UNAUTHORIZED ACCESS

8. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras. Among other things:

    a. since at least April 2010, respondent has transmitted user login credentials in clear, readable text over the Internet, despite the existence of free software, publicly available since at least 2008, that would have enabled respondent to secure such transmissions;

    b. since January 2011, respondent has stored user login credentials in clear, readable text on a user's mobile device, despite the existence of free software, publicly available since at least 2008, that would have enabled respondent to secure such stored credentials;

    c. since at least April 2010, respondent has 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;

    d. since at least April 2010, respondent has failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its IP cameras. Among other things, respondent, either directly or through its service providers, failed to:

        i. 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 for the IP camera, through measures such as:

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

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

            3. 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

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

RESPONDENT'S BREACH

9. As a result of the failures described in **Paragraph 8**, respondent has subjected its users to a significant risk that their sensitive information, namely the live feeds from its IP cameras, will be subject to unauthorized access. As a result of the failures described in **Paragraph 8(d)**, from approximately April 2010 until February 7, 2012, the DVSA setting, described in **Paragraph 5**, did not function properly for twenty models of respondent's IP cameras. (*See* Appendix A, listing the affected models.) In particular, the DVSA setting failed to honor a user's choice to require login credentials and allowed all users' live feeds to be publicly accessible, regardless of the choice reflected by a user's DVSA setting and with no notice to the user.

10. Hackers could and did exploit the vulnerability described in **Paragraph 9**, to compromise hundreds of respondent's IP cameras. Specifically, on approximately January 10, 2012, a hacker visited respondent's website and reviewed the software that respondent makes available for its cameras. The hacker was able to identify a web address that appeared to support the public sharing of users' live feeds, for those users who had made their feeds public. Because of the flaw in respondent's DVSA setting, however, the hacker could access all live feeds at this web address, without entering login credentials, even for users who had not made their feeds public. Thereafter, by typing the term "netcam" into a popular search engine that enables users to search for computers based on certain criteria, such as location or software, the hacker identified and obtained IP addresses for hundreds of respondent's IP cameras that could be compromised. The hacker posted information about the breach online; thereafter, hackers posted links to the live feeds for nearly 700 of respondent's IP cameras. Among other things, these compromised live feeds displayed private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities. The breach was widely reported in news articles online, many of which featured photos taken from the compromised live feeds or hyperlinks to access such feeds. Based on the cameras' IP addresses, news stories also depicted the geographical location (*e.g.*, city and state) of many of the compromised cameras.

11. Respondent learned of the breach on January 13, 2012, when a customer who had read about the breach contacted respondent's technical support staff to report the issue. Shortly thereafter, respondent made available new software to eliminate the vulnerability, and encouraged users to install the new software by posting notices on its website and sending emails to registered users.

THE IMPACT OF RESPONDENT'S FAILURES ON CONSUMERS

12. As demonstrated by the breach, respondent's failures to provide reasonable and appropriate security led to a significant risk that users' live feeds would be compromised, thereby causing significant injury to consumers.

13. The exposure of sensitive information through respondent'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 and conversations or those of their family members, including young children, will be observed and recorded by strangers over the Internet. This risk 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 feeds or images and conversations from business properties). Consumers had little, if any, reason to know that their information was at risk, particularly those consumers who maintained login credentials for their cameras or who were merely unwitting third parties present in locations under surveillance by the cameras.

COUNT 1

14. As described in **Paragraph 7**, respondent has represented, expressly or by implication, that respondent has 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.

15. In truth and in fact, as described in **Paragraphs 8-11**, respondent has not taken reasonable steps to ensure that its IP cameras are a secure means to monitor private areas of a consumer's home or workplace. Therefore, the representation set forth in **Paragraph 14** constitutes a false or misleading representation.

COUNT 2

16. As described in **Paragraphs 5 and 7**, respondent has represented, expressly or by implication, that respondent has taken reasonable steps to ensure that a user's security settings will be honored.

17. In truth and in fact, as described in **Paragraphs 8-11**, respondent has not taken reasonable steps to ensure that a user's security settings will be honored. Therefore, the representation set forth in **Paragraph 16** constitutes a false or misleading representation.

COUNT 3

18. As set forth in **Paragraphs 8-11**, respondent has failed to provide reasonable security to prevent unauthorized access to the live feeds from its IP cameras, which respondent offered to consumers for the purpose of monitoring and securing private areas of their homes and businesses. Respondent's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

19. 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 sixteenth day of January, 2014, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL:

COMPLAINT APPENDIX A

1. TV-IP110 (Version A1.xR)
2. TV-IP110W (Version A1.xR)
3. TV-IP110WN (Versions A1.xR & V2.0R)
4. TV-IP121W (Version A1.xR)
5. TV-IP121WN (Versions V1.0R & V2.0R)
6. TV-IP212 (Version A1.xR)
7. TV-IP212W (Version A1.xR)
8. TV-IP252P (Version B1.xR)
9. TV-IP312 (Version A1.xR)
10. TV-IP312W (Version A1.xr)
11. TV-IP312WN (Version A1.xR)
12. TV-IP322P (Version V1.0R)
13. TV-IP410 (Version A1.XR)
14. TV-IP410W (Version A1.xR)
15. TV-IP410WN (Version V1.0R)
16. TV-IP422 (Versions A1.xR & A2.xR)
17. TV-IP422W (Versions A1.xR & A2.xR)
18. TV-IP422WN (Version V1.0R)
19. TV-VS1 (Version V1.0R)
20. TV-VS1P (Version V1.0R)