

FEDERAL TRADE COMMISSION DECISIONS

FINDINGS, OPINIONS, AND ORDERS
JANUARY 1, 2014, TO JUNE 30, 2014

IN THE MATTER OF

TRENDNET, INC.

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

Docket No. C-4426; File No. 122 3090
Complaint, January 16, 2014 – Decision, January 16, 2014

This consent order addresses TRENDnet, Inc.'s claims regarding the security settings of their SecurView products. The complaint alleges that TRENDnet falsely represented 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. The consent 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. The order also 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.

Participants

For the *Commission*: *Andrea V. Arias* and *Laura D. Berger*.

For the *Respondents*: *John L. Sun, Law Offices of John L. Sun*.

Complaint

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.”

Complaint

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.

The screenshot displays the TrendNet web interface for a Wireless Internet Camera Server (TV-IP110W). The interface is in English and shows the 'Basic » User' configuration page. The left sidebar contains navigation links: Live View, Setup, Smart Wizard, Basic (selected), Network, Video, Event Server, Motion Detect, Event Config, Tools, and Information. The main content area is titled 'User Accounts' and contains three user entries: Administrator, General User, and Guest. Each entry has fields for Password, Confirm Password, User Name, and UserList. The Administrator entry has a 'Modify' button. The General User entry has 'Add/Modify' and 'Delete' buttons. The Guest entry has 'Add/Modify' and 'Delete' buttons. At the bottom, there is a 'Direct Video Stream Authentication' section with a checked 'Enable' checkbox and an 'Apply' button. The location is listed as '2008/12/31 17:42:29'.

User Accounts	
Administrator:	Password: Confirm Password: Modify
General User:	User Name: user Password: Add/Modify UserList: user Delete
Guest:	User Name: guest Password: Add/Modify UserList: guest Delete

Direct Video Stream Authentication: ☒ Enable

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.

Complaint

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

Complaint

- 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;

Complaint

- 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

Complaint

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.

Complaint

**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.

Complaint

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.

Complaint

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)

Complaint

Exhibit A




Wireless Internet Camera Server

- Secure your home or office with wireless streaming video
- Mount this compact stylish Internet camera on most surface areas
- Advanced complimentary software supports up to 16 Internet cameras
- Optimal wireless encryption for secure wireless transmissions

INTERNET CAMERAS
TV-IP110W

Exh. A, p. 1 of 2



Protect Your

- Home
- Family
- Property
- Business

IP Camera Networking Solution

Home Monitoring (TV-IP110W)

Family Monitoring (TV-IP110W)

Property Monitoring (TV-IP110)

Business Monitoring (TV-IP110)

Wireless N Gigabit Router (TEW-433GR)

Internet

Cable/DSL Modem

Wireless Internet Camera Server

The Wireless Internet Camera Server transmits real-time high quality video over the Internet wirelessly. View your camera from any Internet connection. Complimentary SecurView camera management software provides advanced monitoring of up to 16 cameras to protect what you value most.

Ce serveur pour caméra Internet sans fil transmet de la vidéo haute qualité en temps réel sur Internet et sans fil. Visualisez les images de votre caméra à partir de n'importe quelle connexion Internet. Le logiciel de gestion de la caméra SecurView fournit gratuitement vous offre des fonctions avancées permettant de contrôler jusqu'à 16 caméras pour mieux protéger ce que vous chérissez le plus.

El servidor de cámara de Internet transmite vídeos en tiempo real de alta calidad por Internet de manera inalámbrica. Visualice su cámara desde cualquier conexión a Internet. El software complementario para la gestión de la cámara SecurView ofrece monitorización avanzada de hasta 16 cámaras para proteger sus bienes más preciados.

Der drahtlose Internet-Kameraserver überträgt hochwertige Videosignale drahtlos in Echtzeit über das Internet. Sie können die Kamerabilder über eine beliebige Internetverbindung anzeigen lassen. Die kostenlose Kameramanager-Software SecurView bietet Ihnen außerdem die Möglichkeit, über bis zu 16 Kameras all das zu überwachen, was Ihnen besonders wichtig ist.

Il Video Server Internet Wireless trasmette in tempo reale video di alta qualità su Internet senza fili. Visualizza la tua telecamera da qualsiasi collegamento a Internet. Un software in omaggio per la gestione della telecamera SecurView fornisce un monitoraggio avanzato fino a 16 telecamere per proteggere quello che voi ritenete più importante.

O Servidor de Câmera Internet Wireless transmite vídeos de alta qualidade em tempo real pela Internet de modo wireless. Visualize sua câmera a partir de qualquer conexão de Internet. O software complementar de gerenciamento de câmeras, SecurView, proporciona monitoramento avançado de até 16 câmeras para proteger o que você valoriza mais.

Беспроводной Интернет-камера-сервер передает беспроводным путем через Интернет высококачественное видео в реальном времени. То, что показывает камера, можно увидеть из любой точки, где есть подключение к Интернету. Дополнительная программа SecurView для управления камерой предлагает дополнительные возможности управления максимум 16 камерами для защиты того, что вам так дорого.

3-Year Warranty

TV-IP110W

Exh. A, p. 2 of 2

Complaint

Exhibit B



TRENDNET 20th Anniversary

SecurView™ Management Software Included

- Motion detection
- Email alerts
- Program recordings
- Manage 16 cameras

1-Way Audio Day / Night SECURITY

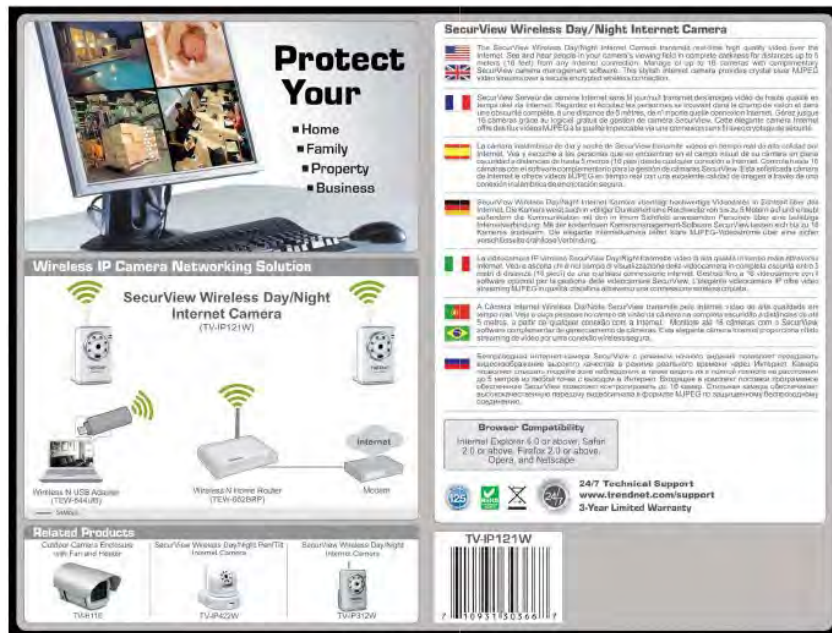
SecurView Wireless Day/Night Internet Camera

- Night vision of up to 5m (16 ft.)
- No need for an Ethernet connection, video is transmitted over a secure encrypted wireless signal
- Program motion detection recording and email alerts with complimentary software
- Mount this compact Internet camera on most surfaces

Powered by an ENERGY STAR® qualified adapter for a better environment

internet cameras
TV-IP121W

Exh. B, p. 1 of 2



Protect Your

- Home
- Family
- Property
- Business

Wireless IP Camera Networking Solution

SecurView Wireless Day/Night Internet Camera (TV-IP121W)

Wireless N Home Router (TEW-632DRP) Internet Modem

Wireless N USB Adapter (TC99-644-001)

Related Products

- Outdoor Camera Extender with Fan and Heater TV-IP11E
- SecurView Wireless Day/Night Internet Camera TV-IP422W
- SecurView Wireless Day/Night Internet Camera TV-IP121W

SecurView Wireless Day/Night Internet Camera

The SecurView Wireless Day/Night Internet Camera transmits high quality video over the internet. See and hear people in your camera's viewing field in complete darkness for distances up to 5 meters (16 feet) from any internet connection. Works up to 16 cameras with complimentary SecurView camera management software. The stylish internet camera provides crystal clear MPEG-4 video transmission & secure encrypted wireless connection.

SecurView Senzor de camera Internet transmite în timp real videoclipuri video de înaltă calitate în timp real de la Internet. Regulați și ascultați la persoanele care înconjură camera în timp real și până la 16 camere prin rețea, numai prin conexiune la Internet. Funcționează până la 16 camere cu programul SecurView gratuit de gestionare a camerei SecurView. Acest elegant camera Internet oferă claritatea video MPEG-4 și o conexiune wireless securizată.

La cámara inalámbrica de día y noche de SecurView transmite vídeo en tiempo real de alta calidad por Internet. Vea y escuche a las personas que se encuentran en el campo visual de su cámara en plena oscuridad en tiempo real desde Internet. Regule y escuche desde Internet a las personas que están a su alrededor. Puede controlar hasta 16 cámaras con el software complementario SecurView. Esta elegante cámara ofrece la claridad de vídeo MPEG-4 y una conexión inalámbrica de vídeo segura.

SecurView Wireless Day/Night Internet Kamera передает видеоклипы в режиме реального времени с Интернета. Вы можете видеть и слышать людей, находящихся в поле зрения камеры, в полной темноте на расстоянии до 5 метров, с любой доступной Интернет. Работает до 16 камер с бесплатным программным обеспечением SecurView. Эта стильная камера обеспечивает четкую картинку MPEG-4 и безопасную беспроводную связь.

La videocamera IP wireless SecurView Day/Night trasmette video in alta qualità internet reale attraverso Internet. Vede e ascolta in tempo reale le persone che si trovano nel campo visuale della videocamera in completa oscurità fino a 5 metri, a partire da qualsiasi اتصال a Internet. Monitora da 16 camere, con il SecurView software complementario per la gestione delle videocamere SecurView. L'elegante videocamera IP offre video streaming MPEG-4 in qualità video sicura per compressione video.

A Camera Internet Wireless Day/Night SecurView transmite vídeo de alta qualidade em tempo real via a rede wireless no campo de visão da câmara em completa escuridão, a distância de até 5 metros, a partir de qualquer conexão à Internet. Monitora até 16 câmeras, com o SecurView software complementar de gerenciamento de câmeras. Esta elegante câmera fornece propagação vídeo MPEG-4 em vídeo seguro com conexão wireless segura.

СекьюрВью интернет камера SecurView с беспроводной передачей видеоклипов в режиме реального времени с Интернета. Вы можете видеть и слышать людей, находящихся в поле зрения камеры, в полной темноте на расстоянии до 5 метров с любой доступной Интернет. Работает до 16 камер с бесплатным программным обеспечением SecurView. Эта стильная камера обеспечивает четкую картинку MPEG-4 и безопасную беспроводную связь.

Browser Compatibility

Internet Explorer 6.0 or above, Safari 2.0 or above, Firefox 2.0 or above, Opera, and Netscape

24/7 Technical Support
www.trendnet.com/support
3-Year Limited Warranty

TV-IP121W

7 109315036017

Exh. B, p. 2 of 2

Complaint

Exhibit C

IP Camera Networking Solution

SecurView Wireless N Day/Night Internet Camera

The SecurView Wireless N Day/Night Internet Camera transmits real-time high-quality video over the Internet. Manage your camera from any Internet connection. Wireless-N technology provides unsurpassed wireless coverage and improved streaming video quality. And this camera is your wireless network's first touch of protection with its Protected Setup (WPS).

La caméra internet journal/nuit sans fil N SecurView transmet des vidéos de haute qualité en temps réel via Internet. Gérer vos caméras Internet depuis n'importe quelle connexion Internet. La technologie sans fil N offre une couverture sans fil sans égal et une qualité de diffusion vidéo améliorée. Ajoutez cette caméra à votre réseau sans fil sécurisé WPS (Wi-Fi Protected Setup) grâce à une seule touche.

La cámara de Internet inalámbrica N SecurView de día y noche transmite en tiempo real vídeos de alta calidad por Internet. Manage sus cámaras de Internet desde cualquier conexión a Internet. La tecnología inalámbrica N ofrece cobertura inalámbrica sin igual así como una mejor calidad de vídeo en tiempo real. Agregue esta cámara a su red inalámbrica con tan solo tocar un botón con tecnología WPS (Wi-Fi Protected Setup).

Das SecurView Wireless-N Internetkamera für Tag- und Nacht überträgt übertragshochwertige Videos über das Internet. Verwalten Sie Ihre Kamera von jedem Internetanschluss. Die Wireless-N-Technologie bietet eine beispiellose drahtlose Reichweite und eine deutlich verbesserte Videoqualität. Dank der WPS-Sicherheitstechnologie (WPS) kann sich die Kamera per Tastendruck in Ihr gesichertes Netzwerk integrieren.

La videocamera IP wireless N SecurView trasmette video in alta qualità in tempo reale mediante internet. Gestire la tua videocamera IP da qualsiasi connessione internet. La tecnologia wireless N offre copertura wireless pari a quella della tecnologia video. Aggiung la videocamera alla rete wireless al semplice tocco di un pulsante con la funzione WPS (Wi-Fi Protected Setup).

O Sistema de Câmera Internet Wireless N Diurno e Noturno SecurView transmite para internet vídeos de alta qualidade em tempo real. Você gerencia a câmera IP a partir de qualquer conexão Internet. Tecnologia Wireless N proporciona cobertura wireless insuperável e qualidade máxima de streaming de vídeo. Adicione esta câmera à sua rede wireless através de um único toque com tecnologia WPS (Wi-Fi Protected Setup).

Матричная веб-камера SecurView Wireless N с беспроводным доступом передает изображения, передаваемые в реальном времени, в интернет. Камеру можно управлять через Интернет. Технология Wireless N обеспечивает покрытие wireless непревзойденной силы и качества. Добавьте камеру к своей беспроводной сети с помощью технологии WPS (Wi-Fi Protected Setup) всего одним нажатием кнопки.

Related Products

SecurView Wireless N Internet Camera TV-IP1100N

SecurView Wireless N Day/Night Internet Camera TV-IP121WN

SecurView Wireless N Pan/Tilt/Zoom Internet Camera TV-DN100N

SecurView Wireless N Day/Night Pan/Tilt/Zoom Internet Camera TV-IP122WN

Browser Compatibility

Internet Explorer 8.0 or above

Software Compatibility

Windows 7 (32/64-bit), Vista (32/64-bit), XP (32/64-bit)

24/7 Technical Support
www.trendnet.com/support
3-Year Limited Warranty

TV-IP121WN

7 811 211 121 21 2

Exh. C, p. 1 of 1

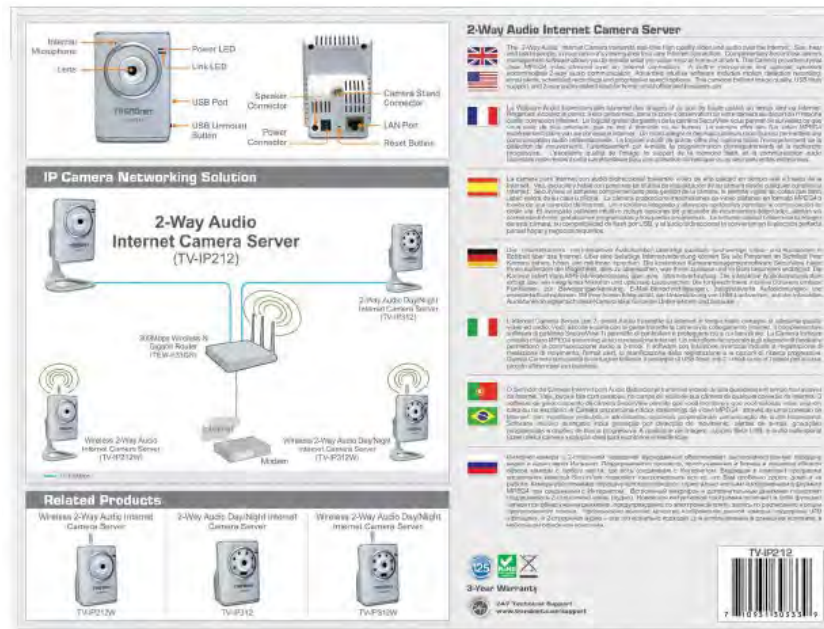
Complaint

Exhibit D

Exh. D, p. 1 of 1

Complaint

Exhibit E



Complaint



The image shows the front of a Trendnet TV-IP212 product box. The box is blue with white and yellow text. At the top is the Trendnet logo, which consists of a stylized 'T' inside a circle. Below the logo, the text 'TRENDNET' is written in a bold, sans-serif font. Underneath that, a yellow banner contains the text '2-Way Audio Internet Camera Server' and 'TV-IP212'. The main body of the box lists features under three headings: 'Hardware', 'Monitoring', and 'Ease of Use'. Each heading is followed by a bulleted list of features. At the bottom left, there is a section titled 'Package Contents' with a bulleted list of items included in the box. On the bottom right, there is a small image of the camera unit itself, which is a small, square, silver-colored device with a lens in the center.

TRENDNET
**2-Way Audio
Internet Camera Server**
TV-IP212

Features

- **Hardware**
 - Built-in USB port allows you to store still images directly onto a USB flash or hard drive.*
 - Supports TCP/IP networking, SMTP Email, HTTP, Samba and other Internet related protocols.
- **Monitoring**
 - High quality MPEG-4 and MJPEG video recording with up to 30 frames per second.
 - Hear and talk to people in your camera's viewing area through your computer.
 - Record streaming video to your computer or Network Storage.
 - Supports still image snapshot to FTP, Email and Flash drive.
 - Motion detection with Email notification.
 - Supports two adjustable motion detection windows with just-in-time snapshot.
 - Supports time stamp overlay.
- **Ease of Use**
 - Quick Universal Plug and Play installation.
 - Free SecurView™ software: view and record up to 16 cameras simultaneously (Windows only).* *

* USB port supports up to a 500mA powered device with FAT16/32 format.
** Monitoring multiple cameras may require a high performance CPU.

Package Contents

- TV-IP212
- Multilingual quick installation guide
- Utility CD-ROM
- Camera stand
- 1.8M (5.9ft) Cat. 5 Fast Ethernet cable
- Power adapter (5VDC, 2.5A)



Exh. E, p. 2 of 2

Complaint

Exhibit F

Exh. F, p. 1 of 1

Complaint

Exhibit G

Exh. G, p. 1 of 1

Complaint

Exhibit H



Exh. H, p. 1 of 1

Complaint

Exhibit I

Exh. I, p. 1 of 2

Complaint



Protect Your

- Home
- Family
- Property
- Business

Pan/Tilt Internet Camera Server

USA: The Pan/Tilt Internet Camera Server provides real-time audio surveillance over a large viewing area. Monitor people in your customer's viewing field and manage the camera from any Internet connection. Size range with an Internet camera-memory pan the camera side-to-side at remarkable 330 degrees and tilt up-and-down 100-degrees.

France: Le serveur de caméra Internet Pan/Tilt permet une surveillance en temps réel d'une surface illimitée. Contrôlez les personnes dans le champ de vision de votre caméra à partir de n'importe quelle connexion Internet. Choisissez un champ de vision plus étendu avec une seule caméra, en la faisant pivoter de 330° et en la faisant basculer de 100°.

Spain: El servidor de cámara de Internet "Pan/Tilt" ofrece vigilancia en tiempo real en áreas de visión muy amplias. Controle la forma que en el campo de visión de la cámara y manage la cámara desde cualquier conexión de Internet. Manejable con una cámara de Internet, controle la cámara de forma remota de lado a lado a alrededor hasta 330 grados y mueva de arriba a abajo hasta 100 grados.

Germany: Die Internetkamera mit Schwenk-Kreiselpanor "Pan/Tilt" erlaubt die Überwachung einer großen Bereich in Echtzeit. Die Kontrolle der im Sichtfeld der Kamera anwesenden Personen und die Steuerung des Kameras-Kreisels über eine beliebige Internetverbindung erlauben. Lassen Sie sich nicht entgehen, auch wenn Sie nur eine einzige Internetkamera verwenden. Das Gerät darf sich seitlich um beeindruckend 330 Grad schwenken und in der Höhe um 100 Grad neigen.

Italy: Il server per videocamera IP con funzione pan/tilt (TV-IP410) offre la sicurezza di sorveglianza in tempo reale su una vasta area. Controlla ed entra nel campo di visualizzazione della tua videocamera e gestisci la videocamera da qualsiasi connessione Internet. Controlla un'area più ampia con una sola videocamera IP rispondendo il campo di visualizzazione orizzontale fino a ben 330° e verticale fino a 100°.

Portugal: O Servidor de Câmaras Internet com Pan/Tilt proporciona segurança em tempo real sobre uma vasta área. Monitorize pessoas no campo de visão de sua câmara através à câmara a partir de qualquer conexão com o Internet. Veja mais com uma Câmera Internet - movimente remotamente a Câmera em qualquer ângulo de 330 graus sobre e 100° de altura vertical.

Russia: Беспроводная Интернет камера-сервер с поворотом и перемещением вертикальной плоскости позволяет наблюдать за объектами любой протяженности в режиме реального времени. Наблюдать за происходящим и вносить изменения в управление камерой можно из любой точки саудейства Интернет. Камера может поворачиваться на 330 градусов в горизонтальной и на 100 градусов в вертикальной плоскости, что значительно увеличивает угол обзора любой камеры.

IP Camera Networking Solution

Home Monitoring (TV-IP410)



Family Monitoring (TV-IP410)





Power Monitoring (TV-IP410W)



Business Monitoring (TV-IP410W)



Vireless N Digital Router (TVN-6330R)

Internet Cable/DSL Modem

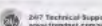
TV-IP410



7 1005150344 15



3 Year Warranty



2007 Technical Support
www.tosonet.com

Complaint

Exhibit J

Exh. J, p. 1 of 1

Complaint

Exhibit K

**Security Video
On The Go**

A woman in a white tank top and blue shorts holds up a smartphone displaying a live video feed of a baby in a crib. In the foreground, a white Trendnet SecurView Wireless N Day/Night Pan/Tilt/Zoom Internet Camera (TV-IP422WN) is shown. The background is a blurred indoor setting.

**SecurView Wireless N Day/Night
Pan/Tilt/Zoom Internet Camera
TV-IP422WN**

- Wireless N technology assures crystal clear streaming video
- Pan 330° side-to-side and tilt 105° up-and-down from any Internet connection
- Program motion detection recording and email alerts with complimentary software
- SecurView Mobile Application allows you to stay in touch while on the go

TRENDNET

Exh. K, p. 1 of 1

Complaint

Exhibit L

Security on the Go

Headquarters

SecuView Wireless N Day/Night Pan/Tilt/Zoom Internet Camera
TV-IP422WN

- Night vision of up to 30 ft (10 ft)
- High speed wireless connection

Mix & Match

Free Software

Free App

TRENDNET

The advertisement features a woman in a dark blazer holding a smartphone that displays a live security camera feed. In the background, a man in a white lab coat is working in a server room. A green beam of light connects the phone to a white Trendnet camera. Below the main image, there are three sections: 'Mix & Match' showing various camera models (TV-IP110WN, TV-IP121WN, TV-IP140WN, TV-IP422WN), 'Free Software' showing a computer monitor with security software, and 'Free App' showing a tablet and a smartphone displaying the app interface. The Trendnet logo is at the bottom right.

Exh. L, p. 1 of 1

Complaint

Exhibit M

The advertisement features the Trendnet logo at the top left. Below it, the headline "Security Video in Your Hands" is written in large, bold, yellow letters. The central image shows a man in a suit holding a smartphone that displays a live security camera feed of a warehouse. To the right of the man, there is a smaller inset image of a warehouse interior with a forklift and a security camera mounted on a shelf. Below the main image, a section titled "Mix & Match" displays a row of six different Trendnet security camera models, each with a yellow double-headed arrow connecting it to the next one. The models are labeled as follows: TV-P110WN, TV-P121WN, TV-IP58P, TV-IP112WN, TV-IP110WN, and TV-IP122WN. At the bottom right, the Trendnet logo is repeated. In the bottom left corner, there is a small copyright notice: "©2011 Trendnet. All rights reserved."

Exh. M, p. 1 of 1

Decision and Order

DECISION AND ORDER

The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from 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 hereby issues its complaint, makes the following jurisdictional findings, and enters the following Decision and Order (“Order”):

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

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

- A. “Affected Consumers” shall mean persons who purchased and installed one of the following Cameras with software last updated prior to February 7, 2012: TV-IP110 (Version A1.xR); TV-IP110W (Version A1.xR); TV-IP110WN (Version A1.xR); TV-IP110WN (Version V2.0R); TV-IP121W (Version A1.xR); TV-IP121WN (Version V1.0R); TV-IP121WN (Version V2.0R); TV-IP212 (Version A1.xR); TV-IP212W (Version A1.xR); TV-IP252P (Version B1.xR); TV-IP312 (Version A1.xR); TV-IP312W (Version A1.xr); TV-IP312WN (Version A1.xR); TV-IP322P (Version V1.0R); TV-IP410 (Version A1.XR); TV-IP410W (Version A1.xR); TV-IP410WN (Version V1.0R); TV-IP422 (Versions A1.xR/A2.xR); TV-IP422W (Versions A1.xR/A2.xR); TV-IP422WN (Version V1.0R); TV-VS1 (Version V1.0R); and TV-VS1P (Version V1.0R).
- B. “App” or “Apps” shall mean any software application or related code developed, branded, or provided by respondent for a mobile device, including, but not limited to, any iPhone, iPod touch, iPad, BlackBerry, Android, Amazon Kindle, or Microsoft Windows device.
- C. “Cameras” shall mean any Internet Protocol (“IP”) camera, cloud camera, or other Internet-accessible camera advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits, or allows for

Decision and Order

the transmission of Live Feed Information over the Internet.

D. “Clear(ly) and prominent(ly)” shall mean:

1. In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
2. In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
3. In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and
4. In all instances, the required disclosures (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.

E. “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 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

Decision and Order

Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

- F. “Covered Device” shall mean: (1) any Internet-accessible electronic product or device, including but not limited to “Cameras,” advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits or allows for the transmission of Covered Information over the Internet; and (2) any App or software advertised, developed, branded, or provided by respondent or any corporation, subsidiary, division or affiliate owned or controlled by respondent used to operate, manage, access, or view the product or device.
- G. “Covered Device Functionality” shall mean any capability of a Covered Device to capture, access, store, or transmit Covered Information.
- H. “Covered Information” shall mean individually-identifiable information from or about an individual consumer input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as a user identifier or screen name; (d) photos; (e) videos; (f) pre-recorded and live-streaming audio; (g) an IP address, User ID or other persistent identifier; or (h) an authentication credential, such as a username or password.
- I. “Live Feed Information” shall mean video, audio, or audiovisual data.
- J. Unless otherwise specified, “respondent” shall mean TRENDnet, Inc., and its successors and assigns.

Decision and Order

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, other device, or an affiliate owned or controlled by respondent, in or affecting commerce, shall 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 Covered Device Functionality;
 - 2. The security, privacy, confidentiality, or integrity of any Covered Information; and
- B. 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.

II.

IT IS FURTHER ORDERED that respondent shall, 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 that could result in unauthorized access to or use of Covered Device Functionality, 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. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device Functionality or Covered Information, including:

- A. The designation of an employee or employees to coordinate and be accountable for the security program;

Decision and Order

- B. The identification of 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 assessment of the sufficiency of any safeguards in place to control these risks;
- C. The identification of 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 respondent's possession or is input into, stored on, captured with, accessed, or transmitted through a Covered Device, 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 should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports;
- E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security 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 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;

Decision and Order

- 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 establish and implement, and thereafter maintain, appropriate safeguards consistent with this Order; and
- H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by Subpart F, any material changes to the 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 its security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this Order, respondent shall 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 shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Covered Devices or other similar 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 Covered Devices or other similar Internet-accessible consumer-grade devices; or a similarly qualified person or organization; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall 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 shall:

Decision and Order

- A. Set forth the specific administrative, technical, and physical safeguards 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 Functionality or 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 Device Functionality and the security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall 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 shall 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 Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRENDnet, Inc.*, FTC File No. 1223090, Docket No. C-4426. *Provided, however*, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

Decision and Order

IV.

IT IS FURTHER ORDERED that respondent shall:

- A. Notify Affected Consumers, clearly and prominently, that their Cameras had a flaw that allowed third parties to access their Live Feed Information without inputting authentication credentials, despite their security setting choices; and provide instructions on how to remove this flaw. Notification shall include, but not be limited to, each of the following means:
1. On or before ten (10) days after the date of service of this Order and for two (2) years after the date of service of this Order, posting of a notice on its website;
 2. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who complain or inquire about a Camera; and
 3. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who register, or who have registered, their Camera with respondent; and
- B. Provide prompt and free support with clear and prominent contact information to help consumers update and/or uninstall a Camera. For two (2) years after the date of service of this Order, this support shall include toll-free, telephonic and electronic mail support.

V.

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

Decision and Order

- A. For a period of five (5) 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; and
 - 2. 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 shall deliver a copy of this Order to all (1) current and future subsidiaries, (2) current and future principals, officers, directors, and managers, (3) current and future employees, agents, and representatives having responsibilities relating to the subject matter of this Order, and (4) current and future manufacturers and service providers of the Covered Products. Respondent shall deliver this Order to such current subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after service of this Order, and to such future subsidiaries, personnel, manufacturers, and service providers 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 shall be at

Decision and Order

least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondent shall 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 shall 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 shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRENDnet, Inc.*, FTC File No. 1223090, Docket No. C-4426. *Provided, however,* that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this Order, shall 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 shall submit an additional true and accurate written report.

Analysis to Aid Public Comment

IX.

This Order will terminate on January 16, 2034, 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 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, an agreement containing a consent order applicable to TRENDnet, Inc. ("TRENDnet").

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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)

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

AB ACQUISITION, LLCCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT AND
SECTION 7 OF THE CLAYTON ACT*Docket No. C-4424; File No. 131 0227**Complaint, December 23, 2013 – Decision, January 28, 2014*

This consent order addresses the acquisition by AB Acquisition, LLC of United Supermarkets, L.L.C. The complaint alleges that the proposed merger, if consummated, would violate Section 7 of the Clayton Act and Section 5 of the Federal Trade Commission Act by removing an actual, direct, and substantial supermarket competitor in Amarillo and Wichita Falls, Texas. The consent order requires Respondent to divest its supermarkets in the two affected markets.

Participants

For the *Commission*: *Chester Choi and Jeremy Morrison.*

For the *Respondents*: *Michael Cutini and Michael E. Swartz, Schulte Roth & Zabel LLP; John Goheen and Matthew J. Reilly, Simpson Thacher & Bartlett LLP.*

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act (“FTC Act”), and by virtue of the authority vested in it by said Acts, the Federal Trade Commission (“Commission”), having reason to believe that AB Acquisition, LLC, a limited liability company, subject to the jurisdiction of the Commission, entered into a merger agreement with United Supermarkets, L.L.C. (“United”), a limited liability company, subject to the jurisdiction of the Commission, in violation of Section 7 of the Clayton Act, as amended, 15 U.S.C. § 18, and Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, and it appearing to the Commission that a proceeding in respect thereof would be in the public interest, hereby issues its Complaint, stating its charges as follows: