1723025

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Maureen K. Ohlhausen
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter

In the Matter of	**DOCKET NO. C-4657**
BLU PRODUCTS, INC., a corporation; and	
SAMUEL OHEV-ZION, individually and as owner and President of BLU PRODUCTS, INC.	

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that BLU Products, Inc., a corporation, and Samuel Ohev-Zion, individually and as an owner and President of BLU Products, Inc. (collectively "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent BLU Products, Inc. ("BLU") is a Florida corporation with its principal office or place of business at 10814 NW 33rd St., Building 100, Doral, Florida 33172.

2. Respondent Samuel Ohev-Zion is a co-owner and the President and CEO of BLU. Individually or in concert with others, Mr. Ohev-Zion controlled or had authority to control, or participated in the acts and practices alleged in this complaint. His principal office or place of business is the same as that of BLU.

3. BLU sells mobile devices to consumers through a number of retailers such as Amazon, Walmart, and Best Buy. To date, Respondents claim to have sold over 50 million devices to consumers around the world. Respondents market BLU as the "fastest growing mobile manufacturer."

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

RESPONDENTS' BUSINESS PRACTICES

5. While BLU describes itself as a "mobile manufacturer," it actually outsources the manufacturing process for the devices it sells to consumers to a number of original device manufacturers ("ODMs").

6. These ODMs manufacture mobile devices branded with the BLU name according to Respondents' instructions and purchase orders. For example, Respondents are responsible for selecting certain software that comes preinstalled on devices, the default settings that consumers first see, and certain security features that are applied to consumers' devices.

7. BLU then sells its customized and branded mobile devices to consumers through a number of retailers, such as Amazon, Best Buy and Walmart.

8. As part of the this process, since at least 2015, in order to provide firmware updating services, BLU licensed software from ADUPS Technology Co., LTD ("ADUPS") and directed ODMs to preinstall this software on Respondents' mobile devices.

9. As a result of BLU directing its ODMs to preinstall ADUPS software on its devices, ADUPS obtained full administrative access and control of Respondents' devices.

10. ADUPS is a China-based company that offers advertising, data mining, and firmware over-the-air ("FOTA") update services to mobile and Internet of Things connected devices. FOTA updates allow device manufacturers to issue security patches or operating system upgrades to devices over wireless and cellular networks.

11. BLU entered into a contract with ADUPS to have the China-based company perform FOTA update services on their devices. Respondents did not ask ADUPS to perform any other services.

RESPONDENTS' DISCLOSURE OF CONSUMERS' PERSONAL INFORMATION

12. Until at least November 2016, the ADUPS software on BLU devices transmitted personal information about consumers to ADUPS servers without consumers' knowledge and consent, including:

- full contents of text messages;
- real-time cellular tower location data;
- call and text message logs with full telephone numbers;
- contact lists; and
- lists of applications used and installed on each device.

13. ADUPS software collected and transmitted consumers' text messages to its servers every 72 hours. ADUPS software also collected consumers' location data in real-time and transmitted this data back to its servers every 24 hours.

14. Reports about this unexpected collection and sharing became public on or about November 15, 2016.

15. After these reports emerged, some consumers concerned about their privacy and security ceased using Respondents' devices entirely. Others expended time and effort disabling the ADUPS software from their devices. In doing so, they have been left with a device unable to receive critical security updates.

16. In order to reassure consumers about the privacy and security of their devices, BLU posted a security notice on its website informing consumers that ADUPS had updated its software to cease its unexpected data collection practices.

17. However, BLU continued to allow ADUPS to operate on its older devices without adequate oversight.

RESPONDENTS' PRIVACY POLICY

18. In its privacy policy, BLU has stated that it limits the disclosure of consumers' information to third parties, as follows:

> We limit the disclosure of your information to only the third parties (e.g. service providers) we use to fulfil[l] our obligations to you. Examples include operating and maintaining our Products, taking orders, delivering packages, sending postal mail and email, removing repetitive information from customer lists, analyzing data, providing marketing consultation and assistance, distributing customer surveys, processing credit card payments, and providing customer service. ***These companies have access to personal information needed to perform their services or functions, but may not use it for other purposes***. (emphasis added)

19. Contrary to the privacy policy, as described in paragraphs 11-17, ADUPS had access to personal information that was not needed to perform FOTA updates, the only service or function BLU contracted with ADUPS to perform. For example, to process FOTA updates, ADUPS did not need to receive contacts or the contents of text messages.

20. BLU's privacy policy has further stated that the company implements:

> appropriate physical, electronic, and managerial security procedures to help protect the personal information that you provide us.

21. In fact, Respondents did not implement appropriate physical, electronic, and managerial security procedures. For example, Respondents failed to implement appropriate security procedures to oversee the security practices of their service providers, such as by:

a. failing to perform adequate due diligence in the selection and retention of service providers; for example, Respondents failed to assess or evaluate the privacy or security practices of ADUPS prior to entering into an agreement with that company;

b. failing to adopt and implement written data security standards, policies, procedures or practices that apply to the oversight of their service providers, including ADUPS;

c. failing to contractually require their service providers to adopt and implement data security standards, policies, procedures or practices; and

d. failing to adequately assess the privacy and security risks of third-party software, such as ADUPS.

22. These failures resulted in the following:

a. ADUPS collected sensitive personal information via BLU devices, without users' knowledge or consent, that ADUPS did not need to perform its functions, as described in paragraphs 11-17.

b. Preinstalled software on BLU devices contained commonly known security vulnerabilities that, for example, made them susceptible to "command injection" attacks, which an unknown third party could exploit to gain full access to users' devices and, among other things, factory reset a device, take screenshots and video recordings of a device's screen, and install malicious applications.

VIOLATIONS OF THE FTC ACT

Deceptive Representation Regarding Disclosure of Personal Information (Count I)

23. Through the means described in Paragraph 18, Respondents have represented, directly or indirectly, expressly or by implication, that they limit the disclosure of users' information to their third-party service providers only to the extent necessary to perform their services or functions on behalf of BLU and not for other purposes.

24. In fact, as described in Paragraph 19, personal information from BLU devices sold by Respondents was transmitted to ADUPS that was not needed to perform their services or functions on behalf of BLU, including FOTA updates. Therefore, the representation set forth in Paragraph 23 is false or misleading.

Deceptive Representation Regarding Data Security Practices
(Count II)

25. Through the means described in Paragraph 20, Respondents have represented, directly or indirectly, expressly or by implication, that they implement appropriate physical, electronic, and managerial security procedures to protect the personal information provided by consumers.

26. In fact, as described in Paragraphs 21-22, Respondents failed to implement appropriate physical, electronic, and managerial security procedures to protect the information provided by consumers. Therefore, the representation set forth in Paragraph 25 is false or misleading.

THEREFORE, the Federal Trade Commission, this sixth day of September 2018, has issued this Complaint against Respondents.

By the Commission.

Donald S. Clark
Secretary

SEAL: