1723025

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Maureen K. Ohlhausen, Acting Chairman**
Terrell McSweeny

In the Matter of	**DOCKET NO. C-**
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 and build

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 co -0.00tleeJ -0.011 Tw [(B)-2 (ara)-2 (e)eces.

a. fa

o

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.