Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of BLU Products, Inc. and Samuel Ohev-Zion, File No. 1723025

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from BLU Products, Inc. ("BLU") and individual Respondent Samuel Ohev-Zion (collectively, "Respondents").

The proposed consent order ("proposed 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 again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

BLU is a mobile device manufacturer that sells smartphone and other mobile devices to consumers through retailers such as Amazon, Walmart, and Best Buy. Samuel Ohev-Zion is an 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 the proposed complaint.

Respondents purchase the smartphones they sell to consumers from Original Device Manufacturers ("ODMs"). ODMs manufacture and customize mobile devices branded with the BLU name based on instructions provided by Respondents. As part of this process, since at least 2015, in order to provide firmware updating services, BLU has licensed software from ADUPS Technology Co., LTD ("ADUPS") and directed ODMs to preinstall this software on Respondents' mobile devices.

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.

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

The Commission's proposed two-count complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act. The first count alleges that Respondents deceived consumers about BLU's data collection and sharing practices by falsely representing in BLU's privacy policy that they limit the disclosure of users' information to third-party service providers only to the extent necessary to perform their services or functions on behalf of BLU and not for other purposes. Contrary to the privacy policy, personal information from BLU

devices sold by Respondents was transmitted to ADUPS that was not needed to perform its services or functions on behalf of BLU, including FOTA updates.

The second count alleges that Respondents deceived consumers about BLU's data security practices by falsely representing that they implemented appropriate physical, electronic, and managerial security procedures to protect the personal information provided by consumers. The proposed complaint alleges that Respondents did not implement appropriate physical, electronic and managerial security procedures. For example, the proposed complaint alleges that Respondents failed to implement appropriate security procedures to oversee the security practices of their service providers, such as by: (1) failing to perform adequate due diligence in the selection and retention of service providers; (2) failing to adopt and implement written data security standards, policies, procedures or practices that apply to the oversight of their service providers; (3) failing to contractually require their service providers to adopt and implement data security standards, policies, procedures or practices; and (4) failing to adequately assess the privacy and security risks of third-party software, such as ADUPS.

The proposed order contains provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Part I of the proposed order prohibits Respondents from misrepresenting: (1) the extent to which they collect, use, share, or disclose any personal information; (2) the extent to which consumers may exercise control over the collection, use, or disclosure of personal information; and (3) the extent to which the implement physical, electronic, and managerial security procedures to protect personal information.

Part II of the proposed order requires Respondents to establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to: (1) address security risks related to the development and management of new and existing covered devices, and (2) protect the security, confidentiality, and integrity of personal information. The program must be fully documented in writing and must contain administrative, technical, and physical safeguards appropriate to Respondents' size and complexity, the nature and scope of Respondents' activities, and the sensitivity of the covered device's function or the personal information.

Part III of the proposed order requires Respondents to obtain an assessment and report from a qualified, objective, independent third-party professional covering the first one hundred eighty (180) days after issuance of the order and each 2-year period thereafter for 20 years after issuance of the order. Each assessment must, among other things: (1) set forth the administrative, technical, and physical safeguards that Respondents have implemented during the reporting period; (2) explain how such safeguards are appropriate to Respondents' size and complexity, the nature and scope of Respondents' activities, and the sensitivity of the covered device's function or the personal information; (3) explain how the safeguards implemented meet or exceed the protections required by Part II of the proposed order; and (4) certify that Respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered devices and the privacy, security, confidentiality, and integrity of personal information is protected.

Part IV of the proposed order requires Respondents, prior to collecting or disclosing any covered information, to: (A) clearly and conspicuously disclose to the consumer, separate and apart from "privacy policy," "terms of use" page, or similar document, (1) the categories of covered information that Respondents collect, use, or share, (2) the identity of any third parties that receive any covered information, and (3) all purposes for Respondents' collection, use, or sharing of covered information; and (B) obtain the consumer's affirmative express consent.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires acknowledgment of the order and dissemination of the order now and in the future to persons with supervisory responsibilities and all employees, agents, and representatives who participate in conducted relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status and mandates that Respondents submit an initial compliance report to the FTC. Part VII requires Respondents to retain documents relating to its compliance with the order for a five (5) year period. Part VIII mandates that Respondents make available to the FTC information or subsequent compliance reports, as requested. Part IX is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

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