

Complaint

IN THE MATTER OF

BLU PRODUCTS, INC.**AND****SAMUEL OHEV-ZION**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. C-4657; File No. 172 3025**Complaint, September 6, 2018 – Decision, September 6, 2018*

This consent order addresses BLU Products, Inc.’s representations regarding consumer privacy and data security. The complaint alleges that Respondents privacy policy represented 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 while, 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. The complaint further alleges that Respondents did not implement appropriate physical, electronic and managerial security procedures. The consent 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.

Participants

For the *Commission*: *Jah-Juin “Jared” Ho* and *Ryan Mehm*.

For the *Respondents*: *Bernard Egozi, Egozi & Bennett, P.A.*

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

Complaint

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;

Complaint

- 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 fulfill[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:

Complaint

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.

Decision and Order

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.

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge Respondents with violation of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

Decision and Order

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission 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 issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:
 - a. Respondent BLU Products, Inc. (“BLU”) is a Delaware corporation with its principal office or place of business at 10814 NW 33rd St., Building 100, Doral, Florida 33172.
 - b. Respondent Samuel Ohev-Zion is an owner and President of BLU Products, Inc. Individually or in concert with others, Mr. Samuel Ohev-Zion formulates, directs, or controls the policies, acts, or practices of BLU Products, Inc. His principal office or place of business is the same as that of BLU.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

- A. “Clearly and conspicuously” means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure (“triggering representation”) is made through only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying

Decision and Order

text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.
 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- B. “Covered Device” means (a) any computing device sold by any Respondent that operates using an operating system, including smartphone, tablet, wearable, sensor, or any periphery of any portable computing device; and (b) the software used to access, operate, manage, or configure a device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or sold by any Respondent, directly or indirectly.
- C. “Covered Information” means the following information from or about a consumer or their device: (a) Geolocation Information; or (b) content of text messages, audio conversations, photographs, or video communications.
- D. “Geolocation Information” means precise location data of an individual or mobile device, including but not limited to GPS-based, WiFi-based, or cellular-based location information.
- E. “Personal Information” means information from or about an individual consumer or Covered Device, including but not limited to: (a) a first and 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 an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social

Decision and Order

Security number; (f) a driver's license or other government-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a "cookie," a mobile device ID, or processor serial number; (j) Geolocation Information; (k) an authentication credential, such as a username and password; or (l) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a Covered Device, including but not limited to network traffic or call log files, contacts, emails, text messages, photos, videos, and audio recordings.

F. "Respondents" means Corporate Respondent and Individual Respondent, individually, collectively, or in any combination.

1. "Corporate Respondent" means BLU, and its successors and assigns.

2. "Individual Respondent" means Samuel Ohev-Zion.

Provisions

I. Prohibition against Misrepresentations about Security and Privacy

IT IS ORDERED that Respondents and Respondents' officers, agents, representatives, employees, and all persons in active concert or participation with any of them, who receive notice of this order, whether acting, directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication the extent to which they protect the privacy, confidentiality, security, or integrity of any Personal Information, including:

- A. the extent to which they collect, use, share, or disclose any Personal Information;
- B. the extent to which consumers may exercise control over the collection, use, or disclosure of Personal Information; and
- C. the extent to which they implement physical, electronic, and managerial security procedures to protect Personal Information.

II. Mandated Data Security Program

IT IS FURTHER ORDERED that Corporate Respondent, and any business that Individual Respondent controls, directly or indirectly, and that collects, maintains, or stores Personal Information, must, no later than the effective date of this order, establish and implement, and thereafter maintain, a comprehensive security program ("Information 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. Such program, the content and implementation of which must be fully documented in writing, must contain administrative,

Decision and Order

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, including:

- A. The designation of an employee or employees to coordinate and be responsible for the Information Security Program;
- B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or unauthorized modification of a Covered Device, 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 Personal Information that could result in the unintentional exposure of such information or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;
- D. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security techniques;
- E. Regular monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- F. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding Personal Information they receive from Respondents, and requiring such service providers, by contract, to implement and maintain appropriate safeguards; and
- G. The evaluation and adjustment of the Information Security Program in light of sub-provisions E-F, any changes to Respondents' operations or business arrangements, or any other circumstances that Respondents know or have reason to know may have an impact on the effectiveness of the Information Security Program.

III. Data Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with the Provision of this Order titled Mandated Data Security Program, Respondents must obtain initial and biennial assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP)

Decision and Order

with experience programming secure 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 Internet-accessible consumer-grade devices; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection.

- B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment, and (2) each 2-year period thereafter for 20 years after issuance of the Order for the biennial Assessments.
- C. Each Assessment must:
 - 1. Set forth the administrative, technical, and physical safeguards that Respondents have implemented and maintained 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 that have been implemented meet or exceed the protections required by the Provision of this Order titled Mandated Data Security Program; 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 and has so operated throughout the reporting period.
- D. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Respondents must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed. Respondents must retain all subsequent biennial Assessments, at least until the Order terminates. Respondents must submit any biennial Assessments to the Commission within 10 days of a request from a representative of the Commission.

IV. Notice and Affirmative Express Consent

IT IS FURTHER ORDERED that Respondents and Respondents' officers, agents, representatives, employees, and all persons in active concert or participation with any of them who receive notice of this order, whether acting directly or indirectly, in connection with any product or service, prior to collecting or disclosing any Covered Information, must:

Decision and Order

- A. clearly and conspicuously disclose to the consumer, separate and apart from any “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 the Covered Information; and
- B. obtain the consumer’s affirmative express consent.

V. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

- A. Each Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 20 years after the issuance date of this Order, Individual Respondent for any business that participates in the marketing or sale of Covered Devices (or similar devices) and that such Respondent, individually or collectively with any other Respondents, is the majority owner or controls directly or indirectly, and the Corporate Respondent, must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC members and managers; (2) all employees, agents, and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which a Respondent delivered a copy of this Order, Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

VI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

- A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:
 - 1. Corporate Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent’s businesses by all of their names, telephone numbers, and physical, postal, email, and Internet

Decision and Order

addresses; (c) describe the activities of each business, including the goods and services offered, and the means of advertising, marketing, and sales and the involvement of any other Respondent (which Individual Respondent must describe if he knows or should know due to his own involvement); (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

2. Additionally, Individual Respondent must: (a) identify all his telephone numbers and all his physical, postal, email and Internet addresses, including all residences; (b) identify all his business activities, including any business for which such Respondent performs services whether as an employee or otherwise and any entity in which such Respondent has any ownership interest; and (c) describe in detail such Respondent's involvement in each such business activity, including title, role, responsibilities, participation, authority, control, and any ownership.
- B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:
1. Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of any Corporate Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
 2. Additionally, Individual Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which such Respondent performs services whether as an employee or otherwise and (ii) any entity in which such Respondent has any ownership interest and over which Respondent has direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.
- C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746,

Decision and Order

such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: In re *BLU Products, Inc.*

VII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Corporate Respondent and Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is a majority owner or controls directly or indirectly, must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;
- D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;
- E. A copy of each widely disseminated representation by Respondents that describes the extent to which it uses or maintains any Personal Information, or protects the privacy, confidentiality, security, or integrity of any Personal Information and the extent to which consumers may exercise control over the collection, use, or disclosure of Personal Information; and
- F. For 5 years from the date received, copies of all subpoenas and other communications with law enforcement, if such communication relate to Respondents’ compliance with this Order.
- G. For 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by

Decision and Order

or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment.

VIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

IX. Order Effective Dates

IT IS FURTHER ORDERED that this Order will be final and effective date upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on September 6, 2038, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than 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 Provision.

Analysis to Aid Public Comment

Provided, further, that if such complaint is dismissed or a federal court rules that the 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 will terminate according to this Provision 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 (“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.

Analysis to Aid Public Comment

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 they 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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**GRIFOLS, S.A.,
AND
GRIFOLS SHARED SERVICES NORTH AMERICA, INC.**

CONSENT 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-4654; File No. 181 0081
Complaint, July 31, 2018 – Decision, September 17, 2018*

This consent order addresses the \$324 million acquisition by Grifols S.A. of Biotest US Corporation. The complaint alleges that the acquisition, if consummated, would violate Section 7 of the Clayton Act and Section 5 of the Federal Trade Commission Act by (1) eliminating actual, direct, and substantial competition between Grifols and Biotest US in three local markets for the collection of human source plasma; (2) increasing the ability of the merged entity unilaterally to decrease donation fees for the collection of human source plasma in each local market; (3) reducing incentives to improve service or quality in each local market for the collection of human source plasma; and (4) increasing the likelihood that Grifols would unilaterally exercise market power in the U.S. market for hepatitis B immune globulin (“HBIG”). The consent order requires Grifols to divest plasma collection centers in three local geographic markets in the United States to Kedplasma LLC, a subsidiary of Kedrion Biopharma Inc. The Order also prohibits Grifols from acquiring any ownership interest in ADMA Biologics, which had been partially owned by Biotest US, without prior notification.

Participants

For the *Commission*: Jean McNeil, Christina Perez and David von Nirschl.

For the *Respondents*: John Ingrassia and Colin Kass, Proskauer Rose LLP.

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act (“FTC Act”), and its authority thereunder, the Federal Trade Commission (“Commission”), having reason to believe that Respondent Grifols, S.A. (“Grifols”), a corporation subject to the jurisdiction of the Commission, has entered into an acquisition with Biotest US Corporation (“Biotest US”), a corporation subject to the jurisdiction of the Commission, in violation of Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, that such acquisition, if consummated, would violate 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:

I. RESPONDENTS

1. Respondent Grifols, is a corporation organized, existing, and doing business under and by virtue of the laws of the Kingdom of Spain with its executive offices and principal place of business located at Avinguda de la Generalitat, 152-158, Parc de Negocis Can Sant Joan, Barcelona, Spain 08174. Its United States address for service of process and the