Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of BLU Products

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 (1) to 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.